Audit Report

OIG-25-028

FINANCIAL MANAGEMENT

Report on the Enterprise Applications' Description of its HRConnect System and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July1, 2024 to June 30, 2025

September 22, 2025

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 22, 2025

MEMORANDUM FOR NICOLAOS B. TOTTEN
DEPUTY CHIEF INFORMATION OFFICER FOR
APPLICATIONS AND DIGITAL SERVICES

FROM: Shiela Michel /s/
Acting Director, Financial Statement Audits

SUBJECT: Report on the Enterprise Applications' Description of its HRConnect System and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2024 to June 30, 2025

We hereby transmit the attached subject report. Under a contract monitored by our office, Saggar & Rosenberg, P.C. (S&R), a certified independent public accounting firm, examined management of the Enterprise Applications' (Enterprise Apps) description of its shared services system for processing customer agencies' human resource transactions titled "Management of Enterprise Applications' Description of its HRConnect System" (the Description) throughout the period July 1, 2024 through June 30, 2025, and the suitability of the design and operating effectiveness of the controls included in the Description. This report includes the Description, management's written assertion, and S&R's independent service auditor's report. The contract required that the examination be performed in accordance with U.S. generally accepted government auditing standards and the attestation standards established by the American Institute of Certified Public Accountants.

In its examination, S&R found in all material respects:

- the Description fairly presents the HRConnect system that was designed and implemented throughout the period July 1, 2024 to June 30, 2025;

- the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2024 to June 30, 2025, and subservice organizations and customer agencies applied the complementary controls assumed in the design of Enterprise Apps' controls throughout the period July 1, 2024 to June 30, 2025; and

- the controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved throughout the period July 1, 2024 to June 30, 2025, if complementary subservice organizations and customer agency controls assumed in the design of Enterprise Apps' controls, operated effectively throughout the period July 1, 2024 to June 30, 2025.

S&R is responsible for the attached independent service auditor's report dated September 18, 2025, and the conclusions expressed therein. We do not express an opinion on Enterprise Apps' description of its controls, the suitability of the design of these controls and the operating effectiveness of controls tested.

If you wish to discuss this report, please contact me at (202) 927-5407.

Attachment

Department of the Treasury
Enterprise Applications

Report on the Enterprise Applications' Description of its HRConnect System and the Suitability of the Design and Operating Effectiveness of Its Controls

For the Period
July 1, 2024 to June 30, 2025

Table of Contents

I: INDEPENDENT SERVICE AUDITOR'S REPORT PROVIDED BY SAGGAR & ROSENBERG, P.C. (S&R)

SAGGAR & ROSENBERG, P.C.
Assurance • Tax • Consulting

Independent Service Auditor's Report

Deputy Inspector General, Department of the Treasury
Deputy Chief Information Officer for Applications and Digital Services

Scope

We have examined management of the Department of the Treasury, Enterprise Applications' (EA) accompanying Description of its HRConnect system for processing customer agencies' human resource transactions throughout the period July 1, 2024 to June 30, 2025 (the Description) and the suitability of the design and operating effectiveness of the controls included in the Description to achieve the related control objectives stated in the Description, based on the criteria identified in "Management of Enterprise Applications' Assertions" (the Assertion). The controls and control objectives included in the Description are those that EA believes are likely to be relevant to customer agencies' internal control over financial reporting, and the Description does not include those aspects of the HRConnect system that are not likely to be relevant to customer agencies' internal control over financial reporting.

The information included in Section V, "Other Information Provided by the Management of Enterprise Applications," is presented by management of the Department of the Treasury, EA to provide additional information and is not part of the Description. Responses from management to findings identified by the service auditor have not been subjected to the procedures applied in the examination of the Description and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description and, accordingly, we express no opinion on it.

EA uses subservice organizations identified in Section III to perform hosting and payroll services respectively. The subservice organizations include Oracle Cloud Infrastructure's Infrastructure-as-a-Service (OCI IaaS) and the United States Department of Agriculture's National Finance Center (NFC). The Description includes only the control objectives and related controls of EA and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified by EA can be achieved only if complementary subservice organization controls assumed in the design of EA's controls are suitably designed and operating effectively, along with the related controls at EA. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary customer agency controls assumed in the design of EA's controls are suitably designed and operating effectively, along with related controls at EA. Our examination did not extend to such complementary customer agency controls, and we have not evaluated the

suitability of the design or operating effectiveness of such complementary customer agency controls.

Service Organization's Responsibilities

In Section II, EA has provided an Assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. EA is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period July 1, 2024 to June 30, 2025. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a Description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on the criteria in management's assertion;
- assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description;
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved; and
- evaluating the overall presentation of the Description, suitability of the control objectives stated in the Description, and suitability of the criteria specified by the service organization in its Assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of customer agencies and their auditors who audit and report on customer agencies' financial statements and may not, therefore, include every aspect of the system that each individual customer agency may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the Description, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section IV of this report.

Opinion

In our opinion, in all material respects, based on the criteria described in EA's Assertion in Section II of this report:

- the Description fairly presents the HRConnect system that was designed and implemented throughout the period July 1, 2024 to June 30, 2025;
- the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2024 to June 30, 2025, and subservice organizations and customer agencies applied the complementary controls assumed in the design of EA's controls throughout the period July 1, 2024 to June 30, 2025; and
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved throughout the period July 1, 2024 to June 30, 2025, if complementary subservice organizations and complementary customer agency controls, assumed in the design of EA's controls, operated effectively throughout the period July 1, 2024 to June 30, 2025.

Restricted Use

This report, including the Description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of EA, customer agency ofEA's HRConnect system during some or all of the period July 1, 2024 to June 30, 2025, and their auditors who audit and report on such customer agencies' financial statements or internal control over financial reporting and have a sufficient understanding to consider it,

along with other information, including information about controls implemented by customer agencies themselves, when assessing the risks of material misstatement of customer agencies' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Saggar & Rosenberg, P.C.

Saggar & Rosenberg, P.C.

Rockville, MD
September 18, 2025

II: MANAGEMENT OF ENTERPRISE APPLICATIONS' ASSERTION

U.S. Department of the Treasury
Washington, D.C.

09/18/2025

Enterprise Applications' Assertion

We have prepared the accompanying description of the Enterprise Applications' (Enterprise Apps') HRConnect system (the system) for processing customer agencies' human resource transactions throughout the period July 1, 2024 to June 30, 2025 entitled "Management of Enterprise Applications' Description of Its HRConnect System" for customer agencies of the system during some or all of the period July 1, 2024 to June 30, 2025, and their auditors who audit and report on such customer agencies' financial statements or internal control over financial statement reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and customer agencies of the system themselves when assessing the risks of material misstatement of customer agencies' financial statements.

Enterprise Applications uses subservice organizations identified in Section III to perform hosting and payroll services. The subservice organizations include the Oracle Cloud Infrastructure-as-a-Service (OCI IaaS) and the United States Department of Agriculture's National Finance Center (NFC). The description includes only the control objectives and related controls of Enterprise Apps and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively along with the related controls at Enterprise Apps. The description does not extend to controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer agency controls assumed in the design of Enterprise Apps' controls are suitably designed and operating effectively, along with related controls at Enterprise Apps. The description does not extend to controls of the customer agencies.

We confirm, to the best of our knowledge and belief, that:

1) The description fairly presents the system made available to customer agencies of the system during some or all of the period July 1, 2024, to June 30, 2025, for processing their transactions as it relates to controls that are likely to be relevant to customer agencies' internal control over financial reporting. The criteria we used in making this assertion were that the description:
    a) Presents how the system made available to customer agencies of the system was designed and implemented to process relevant customer agency transactions, including, if applicable:
        i) The types of services provided, including, as appropriate, the classes of transactions processed.
        ii) The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for customer agencies of the system.

iii) The information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for customer agencies.

iv) How the system captures and addresses significant events and conditions other than transactions.

v) The process used to prepare reports and other information for customer agencies.

vi) The services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

vii) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary customer agency controls and complementary subservice organization controls assumed in the design of the controls.

viii) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b) Includes relevant details of changes to the system during the period covered by the description.

c) Does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of customer agencies of the system and their user auditors and may not, therefore, include every aspect of the system that each individual customer agency of the system and its auditor may consider important in its own particular environment.

2) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period July 1, 2024 to June 30, 2025, to achieve those control objectives if subservice organizations and customer agencies applied the complementary controls assumed in the design of Enterprise Apps' controls throughout the period July 1, 2025 to June 30, 2025. The criteria we used in making this assertion were that:

a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management of Enterprise Apps.

b) The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

c) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Sincerely,

Nicolaos B. Totten

Digitally signed by Nicolaos B. Totten
Date: 2025.09.18 09:46:55 -04'00'

Signature:
Nicolaos B. Totten
Deputy Chief Information Officer for
Applications and Digital Services
U.S. Department of the Treasury

III: MANAGEMENT OF ENTERPRISE APPLICATIONS' DESCRIPTION OF ITS HRCONNECT SYSTEM

OVERVIEW OF OPERATIONS

This examination only covers the products and services provided by Enterprise Applications (EA) relating to the HRConnect system. EA is one of the organizations that the Office of Personnel Management (OPM) has authorized to manage a federal Human Resources Line of Business (HRLOB). As an HRLOB Shared Services Provider (SSP), the HRConnect system is used by all 10 Treasury bureaus and 32 other government agencies with over 230,000 employees and contractors in total.

The HRConnect system is Treasury's enterprise Human Capital Management (HCM) system. The HRConnect system is based on a combination of web-based solutions built on PeopleSoft commercial-off-the-shelf (COTS) software, which constitutes a Platform as a Service (PaaS) (e.g., general support systems of the HRConnect enclave domains of operating systems and database management support systems (DBMS), and support software).

The HRConnect System supports the common HRLOB processes and provides core HR functionality that is interoperable, portable, and scalable. This shared solution provides automated systems that are configurable to the individual organizations' needs while providing a single solution across the Department and federal landscape. HRConnect Services' core functions include Personnel Action Processing, Bi-directional Payroll Interface, Position Management, Recruit Request, Manager Self Service, Employee Self Service, Federal Activities Inventory Reform (FAIR) Act, Personal Identity Verification Data Synchronization (PDS) and Contractor Management, ePerformance, Outside Employment, and Separating Employee and Contractor Clearance (SEC/SCC). The mission of the HRConnect System is to address common operational needs and imperatives of the Department of the Treasury and other federal agencies in an efficient and innovative manner through shared, scalable, and best-practices-based online solutions. By enabling the retirement of legacy systems and automating and streamlining many aspects of human resources, the HRConnect System facilitates increased efficiency and overall productivity for its customers.

The HRConnect Products and Services Organizational Structure Chart, Figure 1, appears below. HRConnect product and support services fall within the HR Line of Business organization. Within the HR Line of Business there are four directorates that support the HRConnect system, Product Management, Customer Delivery and Experience, Development and Application Services and Talent Management Solutions.

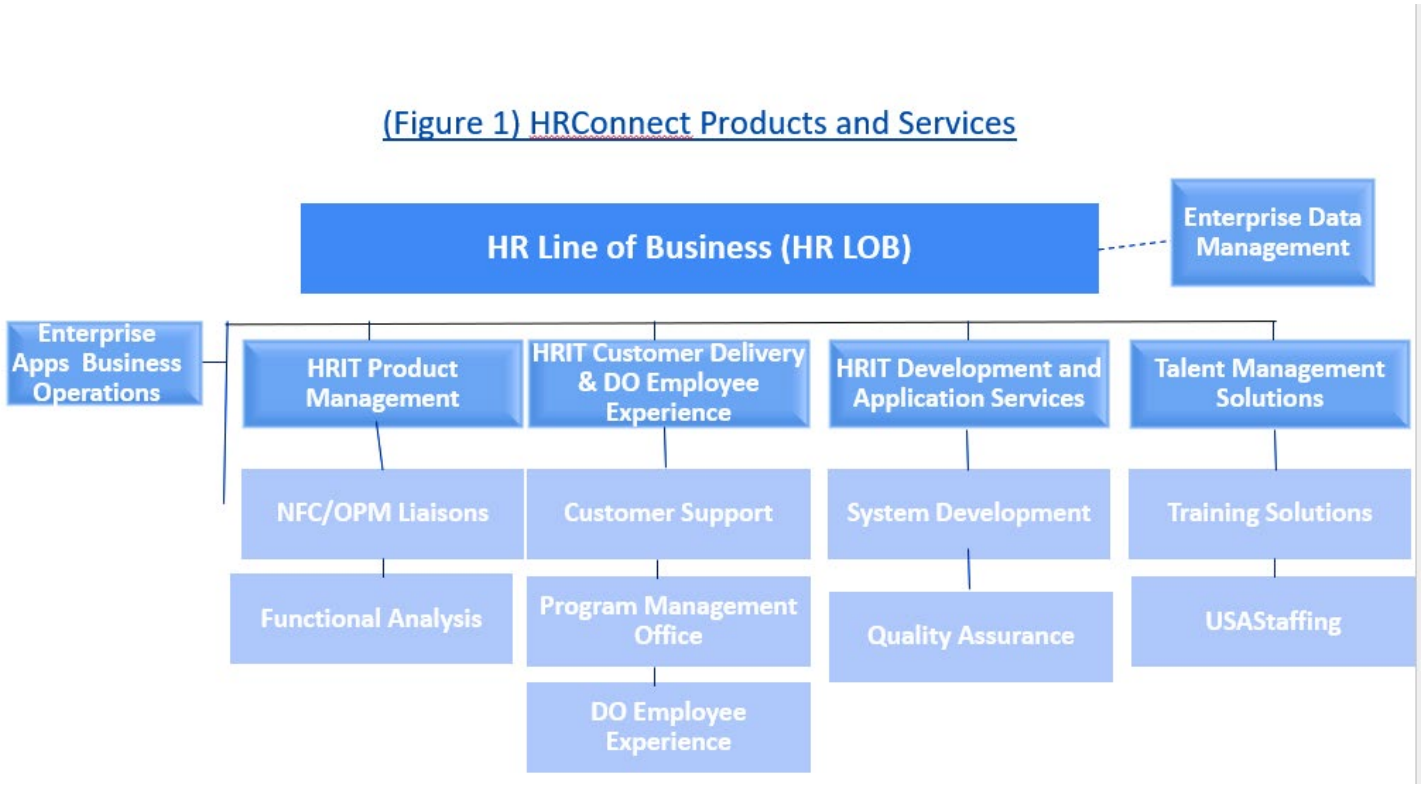


Figure 1: HRConnect Products and Services Organizational Structure

HRConnect

The HRConnect System transforms core back-office Human Resources (HR) functions, moving them from processing-centric paper or legacy systems to a strategic-centric capability enabled through its commercial software underpinning. The HRConnect system is an enterprise web-based HR system that is built on PeopleSoft COTS software and is the foundation of the Treasury Shared Service Center's comprehensive suite of solutions.

Additionally, self-service components of the software fundamentally transform the standard government HR service delivery model, putting additional information, services, and processes (i.e., personal data, position management, requests for personnel action, recruitment, reporting, etc.) directly in the hands of managers, employees, and HR professionals. HRConnect features/functionality include:

List of HRConnect Products and Services:

HRConnect System Features/Functionality	
Manager, Employee and HR Self Service	Personnel Action Requests (the electronic equivalent of an SF-52) may be initiated online by Managers (and/or their Proxies, Detail Managers, or Organizational Delegates) using Manager Self Service. HR staff can process or initiate a full suite of OPM-approved transactions (leveraging 70 different action/reason/update categories) in HRConnect. A Mass Update Module feature is also available to HR to easily process many similar requests with one transaction (realignments, reassignments, etc.). Employees may initiate 12 personnel actions and update 17 different types of personal information, including address, phone number, emergency contact information, as well as the ability to request to retire or resign. In addition, users may view personal information, benefits, and salary, performance and award history.
Personnel Action Requests (PARs)	PARs may be initiated by Managers, their Proxies, Detail Managers, Organizational Delegates and HR specialists. HR staff can process a full suite of OPM-approved transactions (over 190 PAR actions) in HRConnect.
Payroll Interface and Error Correction	Treasury HRConnect features a robust daily bi-directional interface, which transmits personnel, position, and payroll information to the National Finance Center (NFC), Treasury's payroll partner and official System of Record. The reverse interface provides all applied actions, historical corrections, and NFC-generated automatic actions (within-grade increases, etc.) back to the Treasury HR System (HRConnect). This interface allows for error correction (SINQs) directly in Treasury's HRConnect and delivers a comprehensive match solution to keep data synchronized.
Payroll Processing	Treasury HRLOB partners with the NFC to perform all of the payroll related processes as well as other services normally associated with payroll.
Benefits Services	Treasury HRLOB's HR processing partner, Bureau of the Fiscal Service's Administrative Resource Center, provides staff to support the administration of benefits (retirement, life insurance, health insurance, Thrift Savings Plan, Long Term Care Insurance Program, Flexible Spending Account, retirement annuity calculations, and Employee Assistance Program). This is a separate service that Treasury customers may request. Additionally, HRConnect provides convenient access to helpful links to a variety of information, including the National Finance Center's Employee Personal Page, tax calculator, salary tables, TSP information, safety and health programs, and more.
Interfaces to Agency/Bureau and other service provider systems	Treasury's HRConnect provides data feeds to multiple Agency/Bureau systems, including data warehouses, Learning Management Systems, and other service providers. These interfaces can be accomplished through a variety of technical processes.
Workflow and Worklists	Managers and HR Specialists are able to access actions directed to them online for authorization or approval using workflow and worklists. Personnel and other actions are moved automatically through a configurable workflow that includes management authorizations and HR approvals. A sophisticated set of routing rules can be invoked to direct actions by type or location to HR Specialists in that category of action (e.g., awards to budget analysts).
Position Budget Management (PBM)	Treasury's HRConnect provides the ability to manage workforce through position creation, allocation, budgeting, obligation, and incumbency tracking.

HRConnect System Features/Functionality	
Position Budget Management (PBM)	Position Budget Management allows a budgeting office to designate the distinct account code or codes to which the payroll expenses for a specific position will be charged. This function prevents the use of positions for which no account code has been assigned and automates the assignment of new codes as well as the removal of inactivated codes. Automated workflow and system-generated notifications, as well as standard reports and the inclusion of position budget data in the Workforce Analytics reporting system, enable budget analysts to monitor the position budget status of their assigned organizational units and to take actions as needed.
Mass Processing	At times, managers may wish to initiate mass actions that impact a group of employees. Manager Self Service efficiently handles mass awards and mass realignments.
Payroll Documents	HR Specialists have the ability to initiate 30 different payroll documents (e.g., federal, state and local taxes, allotments, health insurance, direct deposits, and health benefits, including several non-federal documents) directly within HRConnect. Afterwards, the HR Specialists will transmit these documents to NFC.
Emergency Contacts	Employees can input an extensive list of emergency contacts. Each emergency contact includes the contact name, address, phone number(s), and relationship to the employee. This information can be accessed and updated at any time, and reports are available to Managers and HR professionals.
Awards Administration	Managers and HR employees may initiate various types of awards (on-the-spot, cash, time-off, etc.) for direct-reporting employees as well as others in the organization. Bureaus can elect to require optional data fields (e.g., accounting code). Administrators have the ability to specify award codes and limits applicable to their agency that are available in a list for managers to initiate and select. This feature includes the ability to initiate mass award actions for many employees.
Separating Employee and Contractor Clearance (SEC/SCC)	Treasury's HRConnect allows online management to initiate the process of clearing an employee or contractor who is separating (e.g., securing issued equipment, security passes, credentials, etc.).
Drug Test Tracking	Treasury's HRConnect provides a way to track the drug testing information.
Employee and Labor Relations, and Third-Party Case Tracking	Treasury's HRConnect provides for tracking of disciplinary cases, grievance cases, and third party (arbitration, etc.) cases. Also allows for tracking negotiation processes between bargaining units and management.
Financial Disclosure Tracking and Reporting	Treasury's HRConnect provides the ability to track employees required to submit Form 278 and 450 financial disclosure forms.
FAIR Act Reporting	Treasury's HRConnect provides the creation and submission of Office of Management and Budget (OMB)-compliant FAIR Act reports.
SF-50's	Treasury's HRConnect provides the capability for employees and HR professionals to access, view, and print SF-50's online, including required email notification to employees of the availability of their SF-50's.
Automated Email Notifications	Treasury's HRConnect automatically sends users notification and reminder emails for NTE dates, career ladder promotion eligibility, SF-50's, worklist items, etc.
Continuity of Operations Tracking	Treasury's HRConnect provides managers the capability of entering and maintaining Continuity of Operations (COOP) group assignments and the skill sets required for bureau/agency continuation of operations for employees.

HRConnect System Features/Functionality	
System Security	Treasury HRLOB's foundational approach to information security for all IT systems developed and managed by this office is a Defense-In-Depth principle implemented as a layered solution. In short, there are multiple defense strategies for multiple targets or initiatives.
Attachments	Treasury's HRConnect provides the ability for Employees, Managers. Proxies, Detail Managers, Organizational Delegates, and HR to attach documentation to actions. Attachment functionality allows approving authorities, reviewers, and processors to easily access and review supporting documentation in order to take immediate action, as necessary. Attachments are available in the following areas: personnel actions initiated by HR or Managers; employee updates (e.g., name change,); recruit requests; Employee/Labor Relations cases; Health Benefit forms; dependent information; and Separation and Home Leave.
Contractor Management	Treasury's HRConnect provides the ability to Contracting Officers to track contracts, task orders, contractors by task order and the type of government furnished equipment supplied to the contractor.
Outside Employment	Treasury's HRConnect provides the ability for employees to submit requests for outside employment to managers for approval. The system captures information related to the business including business type, business name, and estimated hours.
Multi-Factor Authentication (MFA)	HRConnect requires multifactor authentication (MFA) by end users through the use of PIV (Personal Identity Verification) - badge identification and authentication. ID.me and Login.gov are alternative login methods offered to employees on a temporary basis (2 week increments).

Table 1: List of System Features and Functionality

HRConnect Services/Support	
Tier 1 Help Desk Support	Treasury HRLOB partners with the Bureau of the Fiscal Service's Administrative Resource Center (BFS-ARC) to offer Tier 1 Help Desk support. If a customer does not utilize BFS-ARC, then the customer is responsible for providing their own Tier 1 Help Desk support.
Level 2 and Level 3 Customer Support	EA provides Level 2 and Level 3 Customer support in order to respond to questions and manage the applications. The support includes the following features: • Create and run unique operational reports for the customers • Load data for the customers • Manage the application security requests for privileged users • Manage the Bureau Access Detail configuration • Troubleshoot issues submitted by the customers
Business Process Analysis	Treasury's HRConnect specialists assess the customers' current processes and assist in developing future state processes and a plan for implementation. This is based on an analysis done with the organization to ensure that the processes are in alignment with and best utilize the HRConnect technologies.

System Training	Treasury HRLOB offers a 3-day course which provides new HR Specialists with hands-on experience on initiating, routing, and processing HR actions upon request. It reviews the common interfaces and provides understanding of how to process, job requisitions; personnel actions requests; SINQs; cancellation and corrections; and workflow requests. In addition to classroom training, the Treasury HRLOB Training Solutions Team also provides an HRConnect User Manual, job aids, and more. Additionally, there is an established Customer-based Community of Practice group which meets regularly to educate customers on the various features and functions available.

Table 2: List of Products and Services

Relevant Aspects of the Control Environment, Risk Assessment, and

Monitoring *Control Environment*

The control environment is the foundation for all other components of internal control. It provides the discipline and structure, which affects the overall quality of internal control. It influences how objectives are defined and how control activities are structured. EA has established and maintained an environment throughout the organization that sets a positive attitude toward internal control. Through its management, EA has demonstrated a commitment to integrity and ethical values and a commitment to a strong internal control system. EA has established an organizational structure, assigned responsibility, and delegated authority to achieve its objectives. EA is committed to recruit, develop, and maintain competent employees. EA evaluates performance and holds individuals accountable for their internal control responsibilities.

EA is one of Treasury's Government Shared Services Providers and HRConnect is one of the shared offerings. The mission of EA is "To address common operational needs and imperatives of the US Treasury and other federal agencies in an efficient and innovative manner through shared, scalable, and best-practices-based online solutions."

HRConnect employees and contractors are responsible for providing HRConnect system operation and maintenance, which includes the governance and development of changes to the system such as mandatory and regulatory changes, change requests and defect management. Each HRConnect employee has a written position description. All HRConnect employees and contractors with system access receive background investigations and clearance in accordance with Treasury policy. All HRConnect employees and contractors with system access receive mandatory annual training in ethics, privacy, and IT security. Additionally, managers work directly with employees to implement development plans tailored to the employees' needs in work-related topics such as project management, analysis, payroll processing, OPM HR standards, and PeopleSoft Human Capital Management Solutions.

Federal employees follow the *Standards of Ethical Conduct for Employees of the Executive Branch*, which covers the 14 general principles of ethical conduct codified in 5 C.F.R. Part 2635. Annual privacy training is required by Federal Acquisition Regulation (FAR) Subpart 24.3 that addresses the key elements necessary for ensuring the safeguarding of personally identifiable

information for a system of records. In addition, all users of information systems must receive awareness training, as required by the Federal Information Security Modernization Act of 2014 (FISMA).

All HRConnect employees receive an annual performance evaluation. These reviews are based on goals and objectives that are established and reviewed during meetings between the employee and the employee's supervisor. Completed appraisals are reviewed by senior management and become part of the employee's official personnel file.

Risk Assessment

EA conducts risk assessments to identify and manage risks that could affect its ability to provide services to its customers. The process requires team members, project managers, and the management team to identify risks and issues in their areas of responsibilities and to implement appropriate measures and controls to manage these risks. Risks are updated continuously and escalated based on their severity. Additionally, the risk log is analyzed and updated by the Enterprise Applications Cybersecurity (EAC) team and high/critical items are brought for review every two weeks by the entire management team. EA Cybersecurity team has a separate Security Assessment and Authorization (SA&A)/risk assessment process including Plan of Action and Milestones (POA&M) management, which data feeds into the EA project risk management process. The EA Cybersecurity team performs mini-risk assessments throughout the HRC lifecycle; for instance, high-level security impact assessments (SIAs) during the project Intake process and detailed SIAs during the systems change control processes.

Monitoring

Monitoring internal control is a dynamic process that must be adapted continually to manage changing risks. Monitoring of the internal control system is essential in helping internal control remain aligned with changing objectives, environment, laws, resources, and risks. Internal control monitoring assesses the evaluation of the effectiveness of controls over time and promptly resolves the findings from audits and other reviews. EA has established monitoring activities and reacts to events timely with corrective actions. Corrective actions are a necessary complement to control activities in order to achieve objectives.

HRConnect management and supervisory personnel monitor the quality of performance as a normal part of their activities. Management and supervisory personnel inquire of staff and/or review data to ensure the system operates within an effective internal control environment. An example of a key monitoring control is capturing key performance indicators in the monthly Performance Management Review (PMR) report. EA Cybersecurity (EAC) follows the National Institute of Standards and Technology's (NIST's) Risk Management Framework (RMF) for maintaining secure FISMA-compliant systems including the recurring myriad continuous monitoring activities throughout the year.

EA uses Plan of Action and Milestones (POA&Ms) as a tool to document the planned remediation actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. The purpose of HRConnect's

POA&M process is to assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in its programs and systems. POA&Ms delineate resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. At a minimum quarterly, EA reviews POA&M items for consistency with EA risk management strategy and organization-wide priorities for risk response actions.

Information and Communication

HRConnect offers interoperable, portable, and scalable HR/payroll solutions across the federal space. HRConnect core functions include: Personnel Action Processing, Payroll Administration, Benefits Administration, Talent Acquisition, Onboarding, Treasury Learning Management, Integrated Talent Management, Employee and Manager Self Service Portals, and HR transaction processing.

EA uses information to support its internal control system. Information and communication are vital for EA to achieve its control objectives. To support EA risk management decisions, EA has implemented information security monitoring that maintains ongoing awareness of information security posture, vulnerabilities, and threats.

HRConnect Core is based on the PeopleSoft application. The components are PeopleSoft 9.2, Tools 8.60, Oracle 19C database, WebLogic Web/App servers, and Linux 7 running on X86 servers.

EA has established an effective control environment whereby management assesses the risk facing HRConnect as EA seeks to achieve its control objectives. EA applies the NIST RMF to HRConnect, which includes conducting activities related to security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. The High Value Asset (HVA) Assessment can be conducted in lieu of the Security Controls Assessment. EA uses Governance Risk Compliance Certification and Accreditation Module (GRC CAM) to document this process. A NIST Special Publication (SP) 800-30 compliant risk assessment was completed as part of the Security Assessment and Authorization (SA&A) process.

EA performed a formal risk assessment for the HRConnect system as part of the system authorization process. The assessment consisted of internal and external risks that may potentially impact the system. In consideration of risks from the cloud service provider, EA management verified Oracle Cloud Infrastructure (OCI) Infrastructure-as-a-Service's (IaaS's) Federal Risk and Authorization Management Program (FedRAMP) compliance prior to issuing the HRConnect Authority to Operate (ATO). EA management closely monitors OCI IaaS continuous monitoring activities monthly. The activities include the review of system changes, security impacts, any new risks, and remediation actions performed throughout the year by Oracle. EA has defined HRConnect control objectives to enable the identification of risks and define risk tolerances. In the HRConnect program, EA identifies and analyzes risks related to achieve the defined objectives. In addition, EA assesses its risk to be able to respond to significant changes that may impact its internal control system.

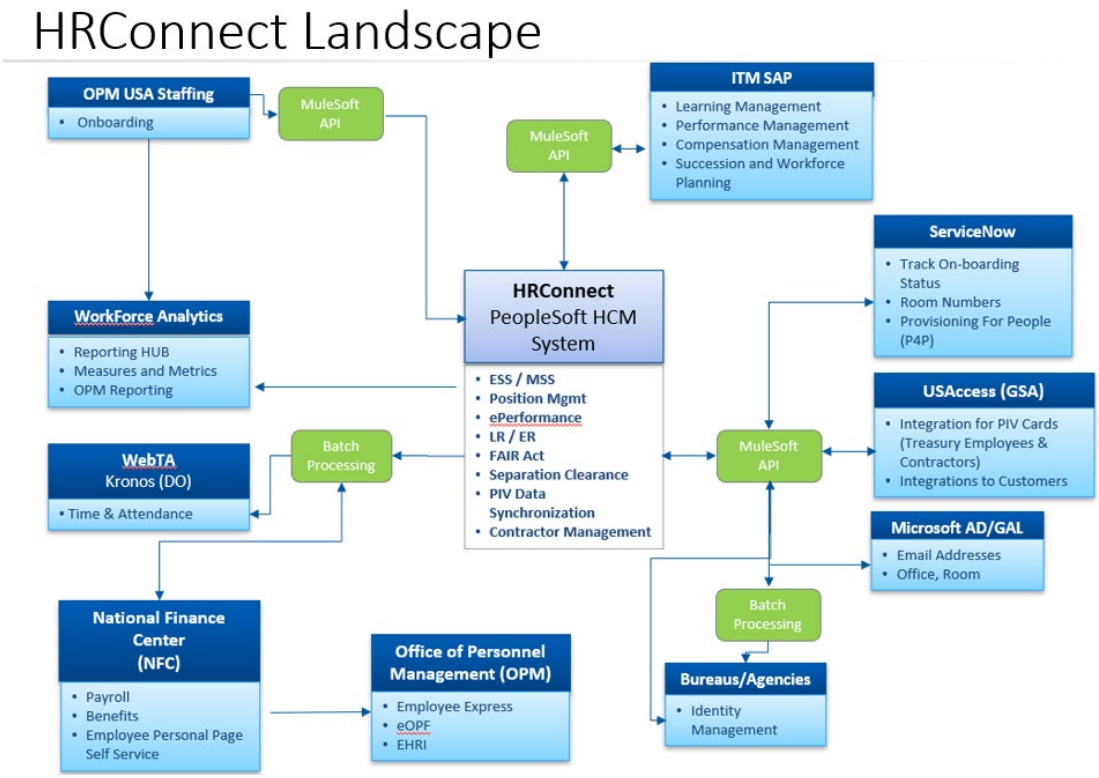
The HRConnect System Security Plan (SSP) provides a summary of the security requirements for the HRConnect system and describes the security controls in place or planned for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. The SSP is viewed as a documentation of structured process of planning adequate, and cost-effective security protection for a system. The HRConnect SA&A package includes security-related documents for the information system such as the SSP, a Federal Information Processing Standards (FIPS) 199 Security Categorization, privacy impact assessment, Security Assessment Results (SAR) report, risk assessment, POA&Ms, Authority to Operate decision letter, contingency plan, configuration management plan, security configuration requirements, and other documents. EA manages the HRConnect SSP and places the plan in the GRC. GRC provides functionality to collect and manage data required by FISMA. GRC features include:

- Ability to track POA&Ms, artifacts, and contacts;
- Permission controlled access to systems; and
- Search by keyword and other parameters.

Systems and Interfaces

EA uses the following systems and interfaces to provide the HRConnect System to federal agencies.

Note: USA Staffing / USA Hire, Integrated Talent Management (ITM) (aside from the interconnection between ITM and HRConnect), and Enterprise Data Management (EDM)/Workforce Analytics systems are not included in this examination.



HRConnect

HRConnect Core is based on the PeopleSoft Human Capital Management application. HRConnect facilitates increased efficiency and overall productivity for its customers. HRConnect Core supports the common HRLOB processes and provides core HR functionality that is interoperable, portable, and scalable. This shared solution provides automated systems that are configurable to each individual organization's needs while providing a single solution across the Department and federal landscape. HRConnect's functions include Employee Self Service, Manager Self Service, HR processing, and bi-directional payroll interface. The data tracked includes, but is not limited to:

- Employee and contractor personal information including data such as name, address, gender, disability, Social Security Number (SSN), salary, etc.;
- Employee skills, education, and certificates;
- Personnel action, including position-related changes and awards;
- Manager and HR workflow approvals and Budget Office position management controls;
- FAIR Act for OMB Reporting;
- Separation Clearance;
- Payroll documents and benefits.

There is a payroll interface that transmits Personnel Action Requests (PAR), Payroll Documents, and Position information to NFC. NFC uses the PAR requests to process payroll. Once customers implement HRConnect, they are able to retire legacy systems as well as automate and streamline many aspects of their HR functions.

The HRConnect, a FISMA High impact categorization system, has full disaster recovery capabilities and implements continuous monitoring for FISMA compliance. System health and the availability are monitored by the Oracle Enterprise Manager (OEM). This monitoring tool sends alerts before issues arise. The Technical Architecture team also monitors the system using cronjobs to alert on various issues. The Security team uses Splunk for event aggregation and monitoring, and other tools as listed below to check all layers of the system.

The security monitoring tools include:

- Nessus/Symantec – Vulnerability scanner (scans any system with an Internet Protocol (IP) address and can recognize multiple systems) to detect vulnerabilities at the operating system and IP layer;
- DBProtect – Vulnerability scanner for databases;
- Trellix – Provides Endpoint Detection and Response (EDR) as well as Data Loss Prevention (DLP);
- WebInspect – Vulnerability scanner for web applications and web interfaces;
- Web Application Firewall (WAF) – Protects against web site hacking attacks;
- Splunk – Collects logs from multiple types of IT systems for correlation and monitoring system activities with alerts; also used for log retention; and
- Microsoft Defender – Anti-Virus software.

Integrated Talent Management (ITM)

Data integration between ITM and HRConnect further ensures accuracy and efficiency by removing the need for manual entry of data into the system for HRConnect customers. Personally Identifiable Information (PII) for Treasury employees regarding their identity and other information described in the Interconnection Security Agreements (ISAs) is established between ITM, HRConnect, and Enterprise Data Management (EDM) programs. Below is a quick summary of the current integrations:

- **ITM Core Data Feed:** An import of Treasury organizational and user date from HRC into the ITM. Additionally, this process provides account creation, modification and reconciliation actions.
- **Control-M Business Intelligence DataMart Feed from SAP NS2 to EDM:** Transfers DataMart files containing Learning Management, Organizational and User data from ITM to the EDM border server for the Internal Revenue Service (IRS), the Office of the Comptroller of Currency (OCC), and Treasury.
- **Monthly Workforce Analytics Import:** A monthly extract of workforce data from EDM which is imported into the ITM Workforce Analytics and Planning data cube.
- **Enterprise Human Resource Integration (EHRI) to OPM:** A monthly export of ITM Learning data delivered to OPM in order to meet EHRI reporting requirements.

Monitoring integrations mentioned above are the shared responsibility of Talent Management System (TMS), and resolution of issues is accomplished with the support and partnership of the accompanying programs. Below in Figure 3 are the different areas of linkage between the EA HRLOB and ITM.

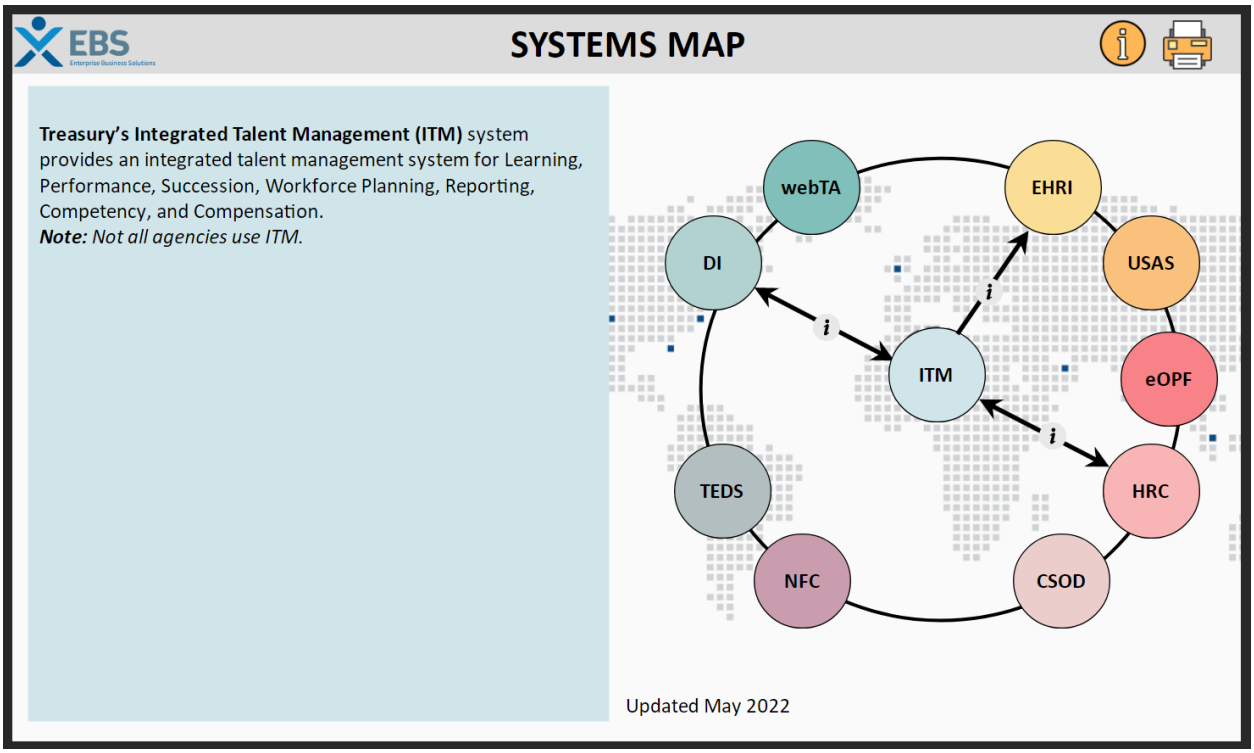


Figure 4: Connect-2-Learn ITM to/From HRC: per Systems Map

Complementary Subservice Organization Controls (CSOCs)

EA's controls relating to the HRConnect system cover only a portion of the overall internal control structure of each customer agency of EA. It is not feasible for the control objectives relating to EA services to be solely achieved by EA. Therefore, each customer agency's internal control over financial reporting must be evaluated in conjunction with EA's controls and related testing detailed in Section IV of this report, considering the complementary subservice organization controls expected to be implemented at the subservice organizations, as described below:

Oracle Cloud Infrastructure's Infrastructure-as-a-Service (OCI IaaS) High GovCloud Cloud Service Provider (CSP)

The OCI IaaS CSP is the primary data center for production and non-production services for HRConnect PaaS and SaaS. The OCI IaaS CSP includes communication, utility and management servers, network cabling, routers, switches, and other communications equipment required to support network connectivity.

United States Department of Agriculture's National Finance Center (NFC)

HRConnect features a daily bi-directional interface transmitting personnel, position, and certain payroll information to the NFC, Treasury's payroll provider. The reverse interface provides all applied actions and NFC-generated automatic actions (annual pay increases, within-grade increases, etc.) back to HRConnect.

List of CSOCs

#	Complementary Subservice Organization Control	Related Control Objective
OCI IaaS CSP		
1	Responsible for assuring that access to computer resources (data, programs, equipment, and facilities) is reasonable based on job responsibilities and segregation of duties principles and restricted to authorized individuals, processes, and devices.	CO 10
NFC		
2	Responsible for assuring that access to computer resources (data, programs, equipment, and facilities) is reasonable based on job responsibilities and segregation of duties principles and restricted to authorized individuals, processes, and devices.	CO 10
3	Responsible for assuring that only valid payroll/personnel transactions are accepted, processed completely and accurately, and reported to customer agencies.	CO 10
4	Responsible for assuring that master data is complete, accurate, and valid.	CO 10

#	Complementary Subservice Organization Control	Related Control Objective
5	Responsible for assuring customer agency requested application changes: authorized customer agencies complete the Form AD-3003, Software Change Request, and submits the request to the Government Employee Service Division (GESD) mailbox for processing.	CO 10
6	When required, customer agencies review and approve the Functional Requirements Document (FRD) and cost estimate for the application change.	CO 10
7	When required, customer agencies participate in User Acceptance Testing (UAT) for application changes	CO 10

Table 3: List of CSOCs

Complementary Customer Agency Controls (CCAC)

EA's controls related to its system processing customer agencies' human resource transactions cover only a portion of overall internal control for each customer of EA. It is not feasible for the control objectives related to EA's services to be achieved solely by EA. Therefore, each customer's internal control over financial reporting should be evaluated in conjunction with EA's controls related tests and results described in Section IV of this report, considering the related CUECs as described below, where applicable. In order for customers to rely on the controls reported on herein, each customer must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

Control Objective 4: Access to Computerized Applications

Customer agencies should establish controls to provide reasonable assurance to properly:

1. Grant access to the systems to users who have been vetted by their organization's security requirements.
2. Provide appropriate levels of privileged user access to the systems to users who have a bona fide need and have met their organization's security requirements; and
3. Assign security roles to users based on their role in the system (e.g., personnel specialists would hold the HR Specialist role vs. a manager who would hold the manager role in HRConnect).

Control Objective 9: Secure Interface Processes

Customer agencies should establish controls to provide reasonable assurance that:

1. The Customer agency's technical contact tests connectivity from the Customer agency's border server to the EA border server using Secure Shell (SSH) and Secure File Transfer Protocol (SFTP).

2. Recommended but not required: The Customer agency's technical contact places the Customer Agency's border server public key on the EA border server so that certificate-based authentication can take place.
3. The Customer agency's technical contact tests file transfers (pushes and pulls) between the Customer agency's border server and the EA border server.

Control Objective 10: Subservice Organizations

Customer agencies should establish controls to provide reasonable assurance that:

1. SINQ errors, Historical Correction and Update Processing (HCUP) status, and mismatch cases are corrected to ensure transactions are processed.
2. The mismatch reports are reviewed and corrected.
3. Authorized customer agencies complete the Form AD-3003, Software Change Request, and submits the request to the GESD mailbox for processing when an NFC software change is applicable.

IV: MANAGEMENT OF ENTERPRISE APPLICATIONS' CONTROL OBJECTIVES AND RELATED CONTROLS, AND S&R's TESTS OF DESIGN AND OPERATING EFFECTIVENESS, AND THE RESULTS OF TESTING

Information Provided by S&R

This report, when combined with an understanding of the controls at customer agencies, is intended to assist auditors in planning the audit of customer agencies' financial statements or customer agencies' internal control over financial reporting and in assessing control risk for assertions in customer agencies' financial statements that may be affected by controls at EA.

Control objective descriptions presented in the following pages were prepared by Treasury EA. This description of controls provided by Treasury EA along with the description of controls presented in Section III represents management's full description of controls.

Our examination was limited to the control objectives and related controls specified by EA in Section III of the report and did not extend to controls in effect at customer agencies.

Each customer agency and its independent auditor are responsible for evaluating this information in conjunction with the internal control over financial reporting at the customer agency in order to assess total internal control. If a customer agency's internal control is not effective, EA's controls may not compensate for such weaknesses.

EA's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by EA. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by EA, we considered aspects of EA's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Test	Description
Inquiry	Inquiry of appropriate personnel and corroboration with management.
Observation	Observation of the application, performance, or existence of a control.
Inspection	Inspection of documents and reports indicating performance of the control.

In addition, as required by paragraph .36 of Attestation Standards – Clarification and Recodification (AT-C) section 205, *Assertion Based Examination Engagements* (American Institute of Certified Public Accountants, Professional Standards), and paragraph .30 of AT-C section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.
Procedures used included:

- Inspecting the source information;

- Inspecting the query, script, and/or parameters used to generate the information; and
- Observing the generation of information.

During our 2025 examination, we identified deficiencies in the EA's controls that we do not consider to be material weaknesses or significant deficiencies. Nonetheless, these deficiencies warrant EA's management's attention. We have communicated these matters to EA's management and, where appropriate, have reported on them separately.

Control Objective 1: System Security Plan

Control provides reasonable assurance that management has established, implemented, and monitored the HRConnect system security plan and disaster recovery plan.

Description of Controls

System Security Plan

The Treasury Department is mandated to comply with Federal Information Security Modernization Act of 2014, Public Law 113–283 (December 18, 2014) which requires agencies to have effective information security controls over information resources to support federal operations, assets and provide a mechanism for improved oversight of agency information security programs.

The HRConnect SSP is the foundation of a security control structure and a reflection of EA's commitment to addressing security risks. The SSP establishes a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

EA has supplemented the Department level controls by implementing specific procedures and controls at the HRConnect applications. EA has followed and documented Treasury Directive (TD) P 85-01, and TD P 15-17, Treasury Shared Services Enterprise Cybersecurity (TSSEC), EA, and HRConnect specific security policies that have been made available to affected personnel, including HRConnect employees and contractors. These policies include system and application rules and expected user behaviors.

The HRConnect SSP provides an overview of the security requirements as it applies to HRConnect, and it describes the controls in place for meeting those requirements. The HRConnect SSP delineated responsibilities and expected the behavior of all individuals who access the system. The EA Enterprise Applications Cybersecurity (EAC) for HRLOB systems (including HRConnect) maintains the HRConnect SSPs and is housed within the ServiceNow GRC.

EA applied NIST RMF to HRConnect, which included conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. EA uses ServiceNow GRC to document this process. *Note: A High Value Asset (HVA) Assessment can be conducted in lieu of the Security Controls Assessment.)*

The security plan establishes security categories for both information contained in HRConnect and the HRConnect application based on Federal Information Processing Standards Publication (FIPS Pub) 199: *Standards for Security Categorization of Federal Information and Information Systems*. EA used FIPS Pub 199 to determine the security categorization risk level of high, moderate, or low. EA selected the controls to implement based on FIPS Pub 200: *Minimum Security Requirements for Federal Information and Information Systems* and NIST SP 800-53 Revision 5: *Security and Privacy Controls for Federal Information Systems and Organizations*. An independent party performs SA&A assessment testing at least annually to determine the extent to which the system's security controls are implemented correctly, operating as intended. The

assessor evaluates management, operational, and technical controls from the detailed Security Requirements Controls Matrix (SRCM). As a result of the SA&A process, findings are analyzed, and a POA&M is created for each control that has failed. When the SA&A is completed, the assessor issues the Security Assessment Reports (SARs). The SAR is performed annually on approximately one-third (1/3) of the security controls, which constitutes a Risk Assessment. The Authorizing Official inspects the SSP, SAR, SRCM, and POA&Ms to determine whether to Authorize to Operate (ATO) for HRConnect. EA maintains and updates SA&A documentation at least annually.

In accordance with the Department's Continuous Monitoring Strategy, a set of controls from NIST SP 800-53 Rev. 5 are defined for system authorization testing annually. The test results are placed in Treasury FISMA Inventory Management System (TFIMS)/GRC by June 30th of every year. HRConnect follows Continuous Monitoring actions throughout the year to review system changes for security impacts. These include monthly and ad-hoc security vulnerability assessment and security configuration scans across the system layers, security impact/risk assessments on system changes, and other continuous monitoring (ConMon) tests.

TFIMS/GRC provides a centralized system for the management artifacts that support assessments, documentation, and reporting on the status of IT security risk assessments and implementation of Federal and NIST standards. TFIMS helps manage and track POA&Ms to include creating, tracking, and closing, as well as automating system inventory and FISMA reporting capabilities. Sufficient evidence must be provided in order to close each POA&M. POA&Ms are utilized to identify any findings, deficiencies, or weaknesses noted in all types of reviews. EA program management, via System Owner (SO), Information System Security Officer (ISSO), Information System Security Manager (ISSM), and Director, Enterprise Applications Cybersecurity (EAC), monitor and track any findings identified in internal and external audits as POA&Ms.

Disaster Recovery Plan

EA developed and maintains a disaster recovery plan for HRConnect. The HRConnect Disaster Recovery Plan complies with the following federal and Treasury policies:

- Federal Information Security Management Act 2002 (FISMA) P.L. 107-347 (Title III of the E-Government Act of 2002), as amended by Federal Information Security Modernization Act of 2014 PL 113-283
- OMB Circular No. A-130 "Managing Federal Information as a Strategic Resource" (07/28/2016)
- Treasury Directive Publication 85-01 'Treasury IT Security Program Vol I (12/12/2016) (TDP 85-01)

The HRConnect Disaster Recovery Plan establishes procedures to recover core, essential HRConnect services following a catastrophic failure at the Oracle GovCloud Primary Site in Ashburn. The following objectives have been established for this plan:

- **Notification/Activation Phase** to detect and assess the situation and, if necessary, activate the plan.
- **Recovery Phase** work with Oracle to bring HRConnect up to operating status at the Oracle GovCloud alternate site in Phoenix.

- **Reconstitution Phase** to restore HRConnect to the Oracle GovCloud Primary Site in Ashburn or new primary facility, if required.

EA conducts a simulation of its disaster recovery procedures on an annual basis. As part of each test, all documentation is reviewed and made current. While specific test scenarios may vary from year to year, a minimum severance of data replication from HRConnect production to the disaster recovery site is performed. We then bring HRConnect services up at the disaster site and verify the applications functionality and its data integrity. At the conclusion of the test, we will take down the DR version of application and restore replication back from production to DR.

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
1.1	Enterprise Applications has documented an application-specific security plan and disaster recovery plan for HRConnect System and has been made available to key stakeholders.	Inquired with EA to obtain an understanding of the process used for updating system security plans. Inspected the relevant policies and procedures associated with system and application to determine they provide an overview of security requirements as it applies to HRConnect. Inspected the latest system security plan to ensure the plan and disaster recovery plan is updated periodically in accordance with their policy and procedures.	**No exceptions noted.**
1.2	An independent party performs on-going assessments at least annually to determine the extent to which the system's security controls are implemented and operating effectively. The HVA (High Value Asset) Assessment can be conducted in lieu of the Security Controls Assessment.	Inquired with EA about the process to complete on-going control assessments as required to determine whether there were any changes made and documented. Inspected the relevant policies and procedures associated with conducting on-going control assessments to determine the frequency of the assessment and the third-party assessor involved in the process. Inspected the most recent security controls assessment performed by the independent assessor to determine controls were assessed on a continual basis in accordance with the policy.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
1.3	Authorizing official (AO) inspects the SSP, SAR, SRCM, and POA&Ms to determine whether to Authorize to Operate (ATO) for HRConnect.	Inquired with the System Manager and EA to obtain an understanding of the Security Assessment and Authorization (SA&A) process. Inspected relevant policies and procedures regarding the SA&A process to determine the process is formally documented. Inspected a complete ATO package to determine the HRConnect system is authorized to operate in the production environment.	**No exceptions noted.**
1.4	An internal team executes a test of HRConnect's disaster recovery procedures at least annually to ensure they are effective at returning HRConnect to an operational state. The results are shared with stakeholders.	Inquired with EA regarding the process for testing disaster recovery procedures to determine how they are ensuring HRConnect can be returned to an operational state. Inspected relevant policies and procedures for disaster recovery testing to determine requirements are defined and documented. Inspected the most recent disaster recovery test and evidence that the results were communicated to stakeholders.	**No exceptions noted.**

Control Objective 2: Security Related Personnel Policies

Controls provide reasonable assurance that security related personnel policies are established, implemented, and monitored, including hiring practices of background investigations, confidentiality agreements, termination, and transfer procedures, IT Cybersecurity Awareness training, and exit interviews, which encompass the returning of property, keys, and removal of logical and physical access.

Description of Controls

On-Boarding and Off Boarding

HRConnect inherits NIST SP 800-53 Rev 5 Personnel Security (PS-1) controls, e.g., background investigation from the *Department of the Treasury Security Manual* (Treasury Department Publication (TD P)) 15-71.

All Treasury EA employees and users with access to Controlled Unclassified Information (CUI), formerly Sensitive But Unclassified Information (SBU) data are restricted to those who have been cleared for an interim clearance and those who have completed and favorably adjudicated background investigations. All approved users who require elevated privileges must complete the Treasury Shared Services Center security online access request, comply with all HRConnect Rules of Behavior and related requirements. Federal employees and contractors/subcontractors who have permission to onboard via interim or full clearance are required to have a completed and favorably adjudicated background investigation that is, at a minimum, compliant with Homeland Security Presidential Directive-12 (HSPD-12) requirements. The HSPD-12 minimum investigation is a National Agency Check with Inquiries (NACI) or such higher-level investigation may be required by the risk level or sensitivity of the position. Individuals lacking Personnel Security approval, regardless of permission levels, will be denied access.

Departmental Offices Employee On-Boarding Procedures include a Provisioning for Personnel (P4P) Request, which assigns Treasury assets. If applicable, Contractors who require a LAN account to Treasury and Treasury assets will also have a P4P Request initiated.

Employee exit procedures, including a Provisioning for Personnel (P4P) Request, are completed to ensure Treasury assets are properly deprovisioned and returned. EA receives Personal Identity Verification (PIV) cards of terminated employees and Treasury deactivates their physical access privileges.

Contractor exit procedures start with a P4P Request being completed by the Contracting Officer's Representative (COR). Departmental Office IT reaches out to the Contractor to coordinate the return of the equipment. Once the equipment is returned, the COR is notified. For PIV card returns, the Contractor can return it physically at 1750 Pennsylvania Ave. (PIV Office), Main Treasury Pass & Lock Office (Room 1015) or mail it back to Access Control.

Training

EA personnel are provided with and required to take IT Cybersecurity Awareness training, Ethics training, Records training, and Privacy Awareness training on an annual basis. EA offers application specific training to HRConnect customers via Connect-2-Learn. Treasury employees and contractors are required to complete and sign Rules of Behavior and confidentiality agreements prior to obtaining access to the Treasury network. New employees are required to complete the IT Cyber Security Awareness training and acknowledge the Departmental Offices Rules of Behavior agreement prior to obtaining access to the Treasury network. Security-related subject matters are regularly emailed to personnel and posted to the internal share drive. EA staff with security-related roles are required to take 4 or 8 hours of security Role-Based Training (RBT) annually.

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
2.1	All Treasury EA employees and users with access to Controlled Unclassified Information (CUI), formerly Sensitive But Unclassified Information (SBU) data are restricted to those who have completed and favorably adjudicated background investigations.	Inquired with the EA to determine types of background investigations required for all employees and contractors who have access to SBU data. Inspected relevant policies and procedures for all employees and users with access to Controlled Unclassified Information to determine that they are in compliance with NIST SP 800-53 Personnel Security requirements. For a sample of employees and contractors who have access to CUI data, verified that they had successfully completed the Treasury Shared Services Center Security Access Request Form and completed a favorable adjudicated background investigation that is compliant with Homeland Security Presidential Directive-12 (HSPD-12).	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
2.2	All EA personnel are required to take IT Cybersecurity Awareness training, Ethics training, Privacy Awareness, and Records training on an annual basis.	Inquired with EA to determine if there are changes or updates in the process for implementing the security awareness program that includes computer-based Cyber Awareness Challenge training. Inspected relevant security and privacy training policies and procedures to determine if there are formal processes in place to document, track, and monitor all EA employee and contractors' training results. Inspected the training materials to determine if there were any updates or changes that have been made and documented. Inspected tracking records to determine training was monitored for staff with system access. For a sample of existing users, inspected training records to determine security awareness training was completed at least on an annual basis.	**No exceptions noted.**
2.3	As part of the employee offboarding process, a Provisioning for Personnel (P4P) Exit Request is submitted to properly deprovision government equipment and revoke privileged accounts in the active directory and the return of property. EA executes P4P. Departmental Office (DO) IT manages the return of the equipment. For Personal Identity Verification (PIV) cards, those are mailed by the Employee or Contractor directly to the Office of Security Programs.	Inquired with EA personnel to verify the offboarding process for both EA employees and contractors is in place. Inspected relevant employee exit procedures to determine EA established and formalized the employee off boarding process. For a sample of terminated employees, determined P4P forms were completed, their PIV cards were deactivated, and their equipment was returned for each one.	**No exceptions noted.**

Control Objective 3: Access to Facilities

Controls provide reasonable assurance that access to facilities is limited to appropriately authorized personnel.

Description of Controls

EA Location

EA's physical location has a security guard located within the lobby of the building requiring the signature of guest and escort by an EA employee. The guest's signature is maintained in a hard copy logbook at the guard station. Access to EA's physical location is controlled using pre-numbered access cards to the elevators and floors. Access cards control access to facilities, as well as the physical access of computer equipment.

Physical access to facilities is gained after an employee/contractor completes the paperwork and fingerprints required for a background investigation. An access badge is issued to a new employee/contractor only after a favorable Special Agreement Check (SAC) is completed. The SAC is a limited investigation (or a series of checks) done only through special agreement between OPM and an agency. Access badges are required for entry and must always be displayed.

Each employee and contractor has an issued PIV card after the appropriate security approval. Employees and contractors must use their PIV cards to access their floors in the elevators and to enter the work area on the floor itself, as well. Signs on floor entrances instruct all personnel to use their badges and not allow others to "piggyback."

PIV Cards

Within the OCIO's Infrastructure and Operations is the Enterprise Systems and Identity Management (ESIM), formerly known as Treasury Enterprise Identity, Credential and Access Management (TEICAM). Its mission is to improve security and efficiency and to promote interoperability through Identity and Access Management for Treasury personnel, organizations, partners, and external agencies including EA's HRConnect. The ESIM provides requirements, coordination, management processes, technical coordination for personal identity verification, credential and access management compliance and solutions for HSPD-12. ESIM and Federal Public Key Infrastructure (PKI) initiatives are established Treasury-wide. ESIM capabilities include: PIV Data Synchronization (PDS); Physical Access Controls (PACs); Logical Access Controls (LACs) for local, remote, and mobile devices, including Derived PIV credential infrastructure and issuance; Multi-Factor Authentication; Federation; Enterprise Identity Management; and PKI. HRConnect does not yet leverage all of ESIM's capabilities.

Oracle OCI IaaS High GovCloud CSP Location

As a Cloud Service Provider under FedRAMP authorization, EAC is not allowed to perform inspections / site visits of CSP sites. However, EA performed an Agency ATO of the OCI IaaS High prior to HRC's Go Live on the platform; reviewing the entire OCI IaaS SA&A package and providing an ATO statement to FedRAMP PMO. HRConnect verified Oracle CSP OCI's FedRAMP compliance prior to the HRConnect ATO, which included validation of the Physical and Environmental (PE) controls of the hosting OCI IaaS platform.

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
3.1	EA's physical location has a security guard located within the lobby of the building requiring the signature of guest and escort by an EA employee. The guest's signature is maintained in a hard copy logbook at the guard station.	Inquired about the security guard in the lobby of the building and where the guest logbook is maintained. Inquired about the logbook containing guest signatures. Inspected the HRConnect SA&A package for the Department of Treasury's implementation status and testing results of inherited NIST SP 800-53 Rev. 5 PE controls from the Oracle OCI IaaS High GovCloud CSP.	**No exceptions noted.**
3.2	Access to EA's physical location is controlled using PIV cards to the elevators and floors. Access cards control access to facilities, as well as the physical access of computer equipment.	Inquired with EA personnel to verify the process for granting the appropriate security level for PIV access is in place. Inspected the HRConnect SA&A package for the Department of Treasury's implementation status and testing results of inherited NIST SP 800-53 Rev. 5 PE controls from the Oracle OCI IaaS High GovCloud CSP.	**No exceptions noted.**
3.3	Each employee and contractor have an issued PIV card after the appropriate security approval.	Inquired with EA personnel to determine the different levels of access and to verify an approval process is in place. For a sample of new employees and contractors, inspected PIV authorizations and issuance statuses to determine PIV cards were issued after the appropriate security approval.	**No exceptions noted.**

Control Objective 4: Access to Computerized Applications

Controls provide reasonable assurance that access to computerized applications and sensitive information is limited to appropriately authorized personnel.

Description of Controls

EA HRConnect system stores PII data and the data is encrypted at rest and in transit. Access to HRConnect system is restricted to users with a valid PIV card, and Multi-Factor Authentication (MFA) for internal to Treasury DO users. Certain federal customers are authenticated via a Treasury Federated Enterprise Identity Credential and Access Management Common Approach to Identity Assurance (CAIA) MFA. Users with access to PII are required to complete the 'TSSC Online Security Access Request', which includes signing a Privileged User Rules of Behavior form. Previously customer UAT testers were required to sign the 'HRConnect Program Office (HRCPO) Agreement to Safeguard Sensitive Data', but that was replaced by 'TSSC Security Access Request' form in Fiscal Year 2021.

For PIV Card users, HRConnect passwords are not used, so they do not expire; PIV PINs changes are inherited from the Treasury PIV; outside of the HRConnect boundary.

Access to HRConnect is dependent on the level of access needed. Non-privileged level access is granted dynamically upon account registration. This includes Employee, Contingent Worker, and Manager basic level access. All managers get access to initiate actions. Managers can assign proxies to initiate, approve, or initiate and approve actions on their behalf. Access privileges are granted based on the level of access required to support the process (e.g., for HR - processor, specialist). Privileged user accounts in production are controlled by strong passwords. Accounts are locked after inactivity. Privileged roles that are no longer needed are manually removed by Customer Service.

Privileged level access can be granted by Bureau Administrators at each customer agency via User Access Maintenance. More advanced privileged-level access and super-level access can only be granted by the EA Customer Service team and requires a Treasury Shared Service Center Online Security Access Request to be completed. Bureau/Sub-agency super and privileged users are created using forms requiring agency and supervisor approval.

The submission of online security access to Customer Service is via Treasury Service Desk Customer Portal, TSSC Online Security Request, or in unique circumstances email to the Customer Service Team E-mail box. The Security Access Request is required for the following access:
* Super User access, which grants users access to all panels and agencies in HRConnect.
* Privileged level access to HRConnect, which includes any roles not available to the agency via Bureau Maintenance User Access Maintenance.
Examples of these roles include, but are not limited to, HR Super role and TR Bureau Super role.

The Treasury Shared Service Center (TSSC) Online Security Access Request is submitted by and signed by the user, the user's manager/bureau representative, and the System Owner or the Bureau can submit on behalf of the user with the signed Rules of Behavior attached to the request through

the approval process. The approved request is then routed to Customer Service to validate and fulfill the request. Customer Service grants the access and notifies the user of the userID and temporary password. Customer Service then notifies the agency that the access has been granted and the user has been provided with their credentials.

User accounts are deactivated via the Personnel Action Request (PARs) process for terminating users. User IDs that have been deactivated due to termination are automatically locked. An automated process runs every night. First, it scans all the PARs for any users that are contingent workers or employees that are no longer active as of that day or prior. The process then updates those user profiles as follows: locks the account, removes the primary permission list, and removes all the roles. This prevents the account from accidentally being unlocked and being usable. Customer Service performs additional audits on user accounts. Privileged and Superuser accounts are analyzed by Customer Service semi-annually to determine which accounts and roles are no longer needed due to termination or transfer.

Health check reports are generated weekly. The health check consists of several reports that are reviewed by Customer Service. Customer Service reviews the health check report to identify user accounts with duplicate IDs. The health check review includes a review of the PAR Approving Officials table for both Terminated users and name changes. The following reports are sent to the agencies to review: Positions that are encumbered by more than one Employee, Active employees reporting to inactive positions, Active employees reporting to inactive DEPTID's, and Inactive Personnel Office ID's on active positions to review and take the necessary action.

The TSSC Online Security Access Request is also used to grant access to the following applications that are included in this audit review:

* Border Server
    - After the online workflow approvals are obtained, Customer Service as the fulfiller, ensures the online access request is complete. Customer Service creates a ClearQuest ticket and uploads a copy of the printed form for action by the Technical Architecture team to set up for Treasury managed environments. The Technical Architecture team communicates the userID and Password to the user. Once the account is set up, Customer Service notifies the requester that the account set up is complete.
* Toad Access
    - After the online workflow approvals are obtained, Customer Service as the fulfiller, ensures the online access request is complete. Customer Service creates a ClearQuest ticket and uploads a copy of the printed form for action by the Technical Architecture team to set up for Treasury managed environments. The Technical Architecture team communicates the userID and Password to the user. Once the account is set up, Customer Service notifies the requester that the account set up is complete. For Oracle Managed environments, the request is submitted, and credentials are provided via My Oracle Support Managed Services Ticketing System.
* ITM Elevated Access
    - The TSSC Online Security Access Request is submitted by and signed by the user, routed to the user’s manager or bureau representative, and the System Owner for approval or the Bureau can submit on behalf of the user with the signed Rules of Behavior attached to the

request through the approval workflow. The approved request is routed to EA Customer Service to validate and fulfill the request for elevated access and then forward them the to the ITM team to complete setup. Access is restricted to users with a valid logon identification and pin. Daily reports are provided to all users who have accessed the system within a specified number of days. Elevated accounts are manually reviewed and reconciled every 90 days.

Complementary Customer Agency Controls

Customer agency auditors should determine whether customer agencies have established controls to provide reasonable assurance to properly grant access to the systems to users who have been vetted by their organization's security requirements. Additionally, it provides reasonable assurance to properly provide appropriate levels of privileged user access to the systems to users who have a business need and have met their organization's security requirements. Finally, customer agency auditors must determine whether customer agencies have established controls to provide reasonable assurance to properly assign security roles to users based on their role in the system (e.g., personnel specialists would hold the HR Specialist role vs. a manager who would hold the manager role in HRConnect.

Remote Access

If remote access is not initially requested as part of the new employee or contractor entry P4P for submission, an EA supervisor sends a request to the Departmental Offices ServiceDesk authorizing employee/contractor's remote access. Once remote access is granted, the employee/contractor can use their workstation to remote access to the same systems they access at their duty station.

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
4.1	Each employee with access to PII has been granted access and complete TSSC Online Security Access Request.	Inquired of EA personnel to determine the process for granting access to HRConnect system. Inspected the relevant access provisioning procedure to determine the process of granting system access is defined and documented. For a sample of new system users, inspected TSSC Security Forms to determine each employee has a completed TSSC Online Security Access Request to grant them authorized access to the system.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
4.2	HRConnect passwords are not used and do not expire. PIV PINs changes are inherited from the Treasury PIV; outside HRConnect boundary.	Inspected a screenshot showing a PIV is required when signing into HRConnect.	**No exceptions noted.**
4.3	Privileged level access that is no longer needed are manually removed by Customer Service.	Inquired with EA management to determine the process for removing privileged access from HRConnect system. Refer to CA 4.1 for our inspection of policies and procedures Inspected results of a comparison between a list of EA separated employees and current active privileged users within the HRConnect system and the database system to determine privileged access that is no longer needed was properly removed by Customer Service.	**No exceptions noted.**
4.4	Privileged user access (including more advanced and Super-level) can only be granted by the EA Customer Service team and requires a TSSC Security Access Request to be completed.	Inquired with EA management to determine the process for granting and removing privileged user access. Inquired with EA management to determine the process for approving the access of Database Administrator (DBA) accounts. Inspected relevant privileged access management policies and procedures to determine requirements for managing privileged user access (including more advanced and Super-level) are defined and documented. For a sample of new users, inspected the Security Access Request Forms to determine the proper approvals are completed and access was granted in accordance with EA requirements.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
4.5	The TSSC Security Online Access Request is used to grant access to the following applications that are included in this audit review: -Border Server -Toad Access	Inquired with EA management to identify the process for granting Border Server, and Toad Access. Refer to CA 4.1 for our inspection of policies and procedures For a sample of Border Server forms, determined the forms are complete and the form was forwarded to the Customer Service team for set up. For a sample of Toad Access Forms, determined if the forms were completed and the form was forwarded to the DBA team for set up.	**No exceptions noted.**
4.6	User accounts are deactivated, automatically locked, and removed for terminated users.	Inquired with EA management to identify the process of managing terminated user accounts. Inspected relevant policies and procedures regarding the user access termination process to verify how terminated users' system accounts are deactivated, locked, and removed from the system. For a sample of separated employees and contractors, obtained and inspected evidence that all separated employees' system accounts are deactivated, locked, and removed as defined in the policy and procedures.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
4.7	Privileged users are reviewed by Customer Service semi-annually.	Inquired with EA management to identify the process of reviewing privileged users. Inspected relevant policies and procedures to determine requirements for periodic review of user accounts are defined and documented. Inspected the evidence of the first semiannual review of privileged user accounts conducted by the Customer Solutions team to determine privileged user access was verified in accordance with EA requirements.	**No exceptions noted.**
4.8	Health check reports are generated weekly and reviewed by Customer Service.	Inquired with EA management to identify the process of reviewing the health check reports. Inspected relevant policies and procedures regarding periodic reviews of health check reports and the review frequency to determine EA has defined and documented requirements for Customer Service review. For a sample of weekly health check reports, reviewed evidence they were conducted by the Customer Service.	**No exceptions noted.**

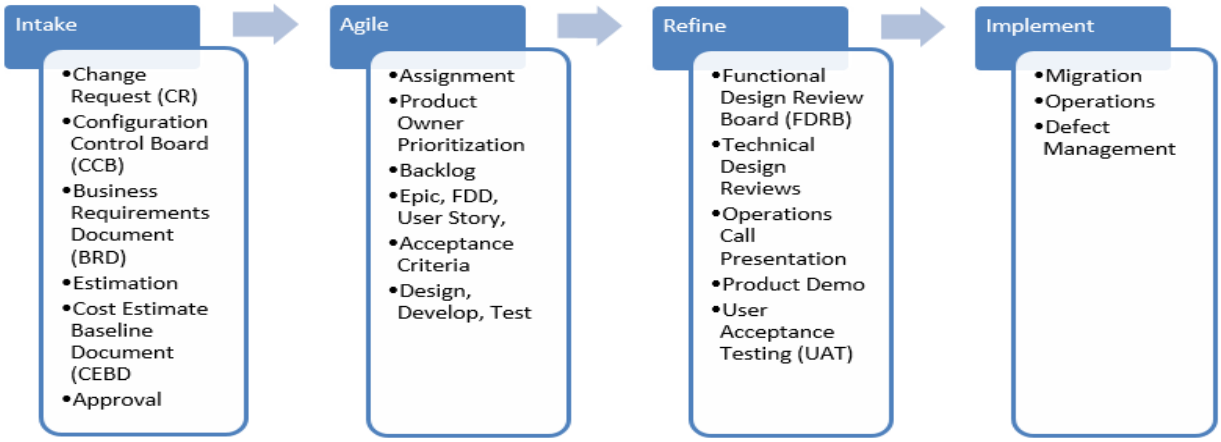
Control Objective 5: Software Development and Maintenance Activities

Controls provide reasonable assurance that software development and maintenance activities are authorized, documented, tested, and approved as described in the HRConnect System Development Life Cycle (SDLC) methodology.

Description of Controls

EA has documented the configuration management process for HRConnect applications that includes roles, responsibilities, reviews, and approvals of configuration changes. The most effective way to protect information and information systems is to integrate security into every step of the system development process, from the intake through implementation.

Our process is defined in four (4) different categories: Intake, Agile, Refine, and Implement.



Intake

Proposed change requests (CRs) or new ideas are submitted by customer representatives or internal team members to the EA Intake Team. The EA Intake Team utilizes the request management module in ServiceNow to manage all incoming requests. This ServiceNow module allows the team to manage the EA Intake process from initial request through turnover to the HRConnect Product Team. Proposed CRs are reviewed weekly by a team of program representatives including functional analysts, project managers, and HRLOB management. During that meeting leadership makes decisions about whether or not to approve the proposed CR to move forward in the process.

The HRConnect Team conducts a monthly Configuration Control Board (CCB) meeting with customer agency/bureau representatives and internal stakeholders, including Enterprise Applications Cybersecurity. During the CCB meeting, the Change Requests are reviewed, and feedback is requested from the customers. The HRConnect Team records the CCB minutes and distributes them to the participants. If the CR is recommended/selected, alternative impacts, both positive and negative, are documented, if appropriate.

If the CR is approved to move forward, a determination is made whether a Business Requirements Document (BRD) should be drafted or if a BRD Waiver is appropriate. BRD Waivers track program management approval to bypass the BRD documentation requirement. The waiver must contain justification for not preparing a BRD and be approved and signed by management (i.e. regulatory, mandatory, low impact, etc.). If a BRD is required for a CR, the team drafts the BRD and obtains approval signatures.

The CR is assigned to an Agile Team for estimation. A cost estimate is completed by the EA Intake Team for the CR based on the BRD and reviewed with program leadership. Program leadership makes a determination if the cost estimate qualifies to be presented to executive leadership during the weekly Project and Portfolio Management (PPM) meeting. If the CR cost estimate is under $10,000 and/or it is in internal facing project with low visibility, a PPM Waiver is completed. The PPM Waiver tracks program management approval to bypass the PPM meeting requirement. The waiver must contain justification and approval signature. Items reviewed at the PPM meeting require an Idea Document, which provides the background of the request and the cost estimate. The Idea Document is presented to executive leadership for approval.

Upon executive approval, EA Intake schedules a conference call with the customer to review the cost estimate. Following that meeting, a Cost Estimating Baseline Document (CEBD) is created. The CEBD summarizes project scope, roles and responsibilities, assumptions, and costs. The CEBD is forwarded to the customer for review and approval signature. Once the customer signs the CEBD and returns it to the EA Intake team, the funding collection process begins (if applicable). Funds are often exchanged via the Inter-Agency Agreement (IAA) modification process. After the IAA modification is developed and executed by both parties and any necessary contracting actions have been completed, the EA Agile Team begins work. The Intake Team moves the project to Execution once a release date is determined. After the release date comes to pass and the project has been implemented, the Intake Team then moves the request from Execution to Complete.

Agile

The Agile Process is a multistep collaborative process that begins with supporting the intake process with estimation and resumes after official project handoff from the EA Intake team. Upon project turnover, the CR is added to the Agile Team's backlog and the Product Owner prioritizes the work. Analysis, design, development, testing, product demos are completed in Sprints and implemented after customers validate changes during a user acceptance test (UAT) period.

EA uses ClearQuest change management software to control changes for HRConnect and to maintain application baselines throughout the process. The change management software manages the approvals, audit trails, coding, testing, and publication of the software changes. The software allows automated workflows and email notifications to ensure that appropriate team members are alerted in near real-time when action is required; and software changes, along with associated requirements, are documented. Change requests are tested according to development organization guidelines and approved prior to implementation.

Refinement

An Epic User Story Functional Design Document (EUSFDD) is drafted and reviewed internally in the Functional Design Review Board (FDRB) meeting with representatives from the Functional, Development, Quality Assurance, Customer Service, and Enterprise Applications Cybersecurity Teams in attendance. Adjustments are incorporated into the document based on internal team feedback. Enterprise Applications Cybersecurity Team provides Security Impact Assessments (SIA) of the CRs identifying risk, security controls impacted and cybersecurity actions. The EUSFDD is ultimately approved by the Director of HRConnect Product Management Team.

An EA Developer performs a Technical Design Document (TDD) review to walk through the changes and impact based on the EUSFDD. The TDD is a working document and is completed at the end of development.

If the CR Level of Effort (LOE) is less than 40 hours (data only update, one-time script, minor text changes to pages, emails, etc.), an EUSFDD and/or TDD Review may not be required. A waiver is completed and submitted for approval by the designated Federal Manager.

The development and technical documentation are considered complete, when the CR includes:

- an EUSFDD or EUSFDD waiver,
- a TDD Review waiver or a TDD Review is conducted.
- a peer review performed as described in the Software Peer Review Check List.

The Agile Teams present and share change request (CR) changes with the customers with product demonstrations and presentations.

Implementation

Once approvals are received, the change is migrated to the production environment by an independent partner.

Each stage/lifecycle is separate for purposes of creating an independent process (intake, design, development, testing, internal validation, and customer user acceptance). At the end of the cycle (whether internal or customer acceptance), approval is required for the changes made.

Customer cybersecurity points of contact are invited to come onsite (virtually) and review the HRConnect SA&A package documentation, typically annually, which often includes information on recent and upcoming major changes to the system.

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
5.1	EA has documented the configuration management procedures for HRConnect. The procedure document defines: • Roles and responsibilities • Requirements for the review and approval of configuration changes.	Inquired with EA personnel to determine how EA has documented the formal configuration management process for HRConnect applications including the frequency of the management review of the procedures document. Inspected relevant policies and procedures for the configuration management process to determine the defined and documented processes included: • Roles, responsibilities, procedures, and documentation requirements for configuration management and systematic policy implementation. • Requirements for the regular review and approval of configuration changes. Also refer to testing performed under Control Number 5.2 through 5.6 related to testing a sample of change requests.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
5.2	All changes to the HRConnect system are authorized, documented, tested, and approved.	Inquired with EA personnel to determine the scope and extent of the change management process including documentation, approval requirements, and to verify a change control board exists. Inspected relevant policies and procedures associated with the change management process to determine the existing change management process from initiation to approval is defined and documented along with a list of CCB members who are responsible for review of all program changes prior to implementation. For a sample of closed change tickets, determined if all changes were authorized, documented, tested, approved, and implemented appropriately.	**No exceptions noted.**
5.3	For approved change requests, determinations are made whether a Business Requirements Documents (BRD) or BRD waiver forms are needed. BRD Waivers track program management approval to bypass the BRD documentation requirement. The waiver must contain justification for not preparing a BRD and be approved and signed by management. If a BRD is required for a change request, the team drafts the BRD and obtains approval signatures.	Inquired with EA personnel to obtain an understanding of the process of determining whether a BRD or a BRD waiver form is required to be created when a change request is approved. Inspected relevant policies and procedures for the BRD/BRD waiver process to determine the process is defined and documented. For all sampled changes from Control Number 5.2, determined whether EA documented and maintained all correspondent approved BRD or BRD waiver forms. In addition, for all waivers, ensured proper justifications are documented within the respective form.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
5.4	Cost estimates are completed for Change Requests based on the associated BRD and are reviewed with program leadership to make a determination if the cost estimate qualifies to be presented to executive leadership during the weekly Project and Portfolio Management (PPM) meeting.	Inquired with EA personnel to obtain an understanding of the process of completing the cost estimates for change requests and the approval process. Inspected relevant policies and procedures to determine the process for completing cost estimates for change requests are documented and approved. For all sampled changes from Control Number 5.2, obtained evidence to determine whether cost estimates are completed and reviewed with program leadership if the cost estimate meet the specific threshold requirement. If the cost estimate did not meet the requirement, ensured the sampled tickets have valid Project and Portfolio Management waivers.	**No exceptions noted.**
5.5	An Epic User Story Functional Design Document (EUSFDD) is drafted, reviewed, and approved. In addition, EA developers perform Technical Design Document (TDD) reviews to walk through the changes and impact based on the EUSFDD.	Inquired with EA personnel about the EUSFDD and the review and approval process during the refinement phase to determine how the EUSFDD life cycle is managed. Inspected relevant policies procedures to determine the EUSFDD review and approval process is defined and documented. For all sampled changes from Control Number 5.2, obtained evidence to determine whether EUSFDD reviews and approvals were completed.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
5.6	Once approvals are received, the change is migrated to the production environment by an independent partner.	Inquired with EA personnel to determine how changes are migrated into production. Inspected relevant policies and procedures on how changes are migrated to the production environment after appropriate approvals to determine EA requirements for change migration and separation of duties are defined and documented. For all sampled changes from Control Number 5.2, obtained evidence to determine whether all changes were moved into production by an independent partner.	**No exceptions noted.**

Control Objective 6: Processes and Procedures to Respond to Unusual Activity or Intrusion Attempts

Controls provide reasonable assurance that management has processes and procedures in place to monitor unusual activity and intrusion attempts.

Description of Controls

EA adheres to guidance from NIST SP 800-53 Revision 5 and U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD)-22-01 and BOD-23-01 for Vulnerability Management. On behalf of a System Owner, ISSO, and ISSM, EA Cybersecurity security engineers conduct a monthly vulnerability assessment, and system security configuration scans to identify vulnerabilities. For HRConnect on Oracle Cloud Infrastructure Cloud Service Provider (OCI CSP), the vulnerability and configuration scans are run on Mondays, Wednesdays and Fridays. EA analyzes the identified vulnerabilities and either mitigates the vulnerability or documents what is required for production processes. EA scans the various layers of HRConnect based on Treasury policy and the EA Cybersecurity team's formal standard operating procedures (SOP). Vulnerabilities are provided to System Owners and Technical staff for remediation.

For HRConnect on Treasury Enterprise Oracle (TEO)/ OCI CSP, monthly scans are conducted by EA cyber engineers and tracked in security scan software's dashboard reports and reports are delivered to Operations for remediation. The EAC's TEO Tenable Instance is integrated with ServiceNow SecOps Vulnerability Response. ServiceNow Vulnerability Response (VR) Module is a vulnerability management solution that enables organizations to identify, prioritize, and remediate vulnerabilities across their IT infrastructure. Vulnerabilities identified from Tenable will generate new issues in ServiceNow and be tracked within the Governance Risk Compliance (GRC) Authorization Packages as Vulnerable Items (VI) and POA&M [Plan of Action and Milestones] (when they become past due). ServiceNow will automatically close the VI and POA&M when the vulnerability is remediated.

EA follows the TSSEC (Treasury Shared Services Enterprise Cybersecurity) timelines for remediation:

- Critical Findings: 15 days
- High Findings: 30 days
- Moderate Findings: 90 days
- Low Findings: 180 days

EA's vulnerability management process follows Departmental policy (TDP 85-01) on Flaw Remediation including patch management and system updates to ensure system flaws are identified, reported, and corrected. Patches are prioritized and approved through EA and are tested on non-production systems prior to migration to and installation on all production systems.

Penetration testing is conducted annually to exploit vulnerabilities and insufficiently configured security controls to determine whether a user could obtain unauthorized access to EA's IT operational environment; specifically, to demonstrate whether technical weaknesses were present

in EA's computer systems that may allow employees or outsiders to inflict harm to, attack, and/or impact HRConnect.

HRConnect collects audit logs from the various HRConnect layers: PeopleSoft application, and supporting operating system and DBMS audit logs. These are consolidated into Splunk centralized repository where dashboards segregate and help identify potential indicators of compromise. Audit logs are reviewed by system admins, ISSO, and ISSM weekly. Audit logging was expanded in December 2023 as part of the OMB Memorandum M-21-31 initiative, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents". Audit logs are also now exported to the Treasury Shared Services Operations Center (TSSOC).

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Operating Effectiveness Testing (S&R)
6.1	For HRConnect on OCI CSP, monthly scans are tracked in security scan software's dashboard reports. Findings are tracked for remediation, and vulnerabilities identified from monthly scans are added as POA&Ms based on policy's remediation schedule.	Inquired with EA personnel regarding the process of conducting monthly scans to determine whether the process is being followed and to verify any changes that have been made are documented. Inspected relevant policies and procedures associated with conducting monthly scans to determine the personnel involved in the process. Inspected monthly scan results to determine they are tracked in the security scan software's dashboard reports. For a sample of findings that were identified in the most recent monthly scans for HRConnect on OCI CSP, determined if POA&Ms were created and tracked through resolution.	**No exceptions noted**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Operating Effectiveness Testing (S&R)
6.2	EA Cybersecurity security engineers conduct a monthly vulnerability assessment and system security configuration scans to identify network vulnerabilities. For HRConnect on OCI CSP, the vulnerability and configuration scans are run on Tuesdays and Fridays. EA analyzes the identified vulnerabilities and either mitigates the vulnerability or documents it is required for production processes.	Inquired with EA personnel to determine the process for conducting vulnerability assessment and system security configuration scans to identify network vulnerabilities. Inspected relevant policies and procedures outlining the process for conducting vulnerability assessment and system security configuration scans to identify network vulnerabilities to determine EA vulnerability management requirements are defined and documented. For a sample of monthly system security configuration scans, reviewed results and, as applicable, obtained supporting documentation that evidences the remediation of identified vulnerabilities.	**Exception Noted – Database Scans (Notification of Finding and Recommendations (NFR) 1)** During the entire period under examination, July 1st 2024 to June 30th 2025, the required DBProtect vulnerability scans were not performed for the seven (7) databases noted in *Enterprise Application Cybersecurity Security Engineering and Operations Vulnerability Management Project Plan* (March 2024) Version 2.0. .
6.3	Penetration testing is conducted annually to exploit vulnerabilities and insufficiently configured security controls to determine whether a user could obtain unauthorized access to EA's IT operational environment.	Inquired with EA personnel to determine the process for conducting penetration testing. Inspected policies and procedures outlining the process for conducting penetration tests on the EA IT operational environment to determine EA penetration testing requirements are defined and documented. Inspected the latest penetration testing result to determine identified risks were properly addressed in accordance with EA requirements.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Operating Effectiveness Testing (S&R)
6.4	HRConnect collects audit logs from the various HRC layers: PeopleSoft application, and supporting operating system and DBMS audit logs. These are consolidated into Splunk centralized repository where dashboards segregate and help identify potential indicators of compromise.	Inquired of EA personnel to determine the process of monitoring unusual activities. Inspected procedures outlining the process for monitoring unusual activities to determine EA's requirements for HRConnect audit logging are defined and documented. Inspected relevant documentation of the Splunk implementation to determine audit logs are collected from HRC's various layers and to verify auditable events are defined for them consistent with EA requirements. Inspected the relevant documentation of the Splunk implementation to determine dashboards are configured to segregate and help identify potential indicators of compromise. Inspected evidence of incident notifications generated from Splunk to ensure the system owner is notified for remediation of any potential concerns in accordance with EA requirements.	**No exceptions noted.**

Control Objective 7: Accuracy Testing Methods

Controls provide reasonable assurance that reconciliations, exception reports, and transmittal process are designed to ensure interfaces are working accurately. For each connection method, HRConnect uses technical methods to validate that the connection is established, and then validates that the data transfer occurs accurately.

Description of Controls

Data Integration with External Applications

HRConnect exchanges data with business partners using three different platforms: Border Server services, Enterprise MuleSoft Application Program Interface (API) services, and Integrated Talent Management.

Border Server

Control-M runs various jobs to push and pull data between the HRConnect border server and business partner systems. With one exception, all of these interfaces are conducted using the SFTP protocol. That exception is the USDA National Finance Center (NFC). Currently, the interface with the NFC only supports the File Transfer Protocol (FTP). However, the NFC is in the midst of moving to SFTP, which HRConnect will adopt as soon as it becomes available.

If critical Control-M interfaces jobs fail, Control-M will send an email and warning page to the on-call DBA. As is appropriate, Control-M will also automatically rerun the file transfer job several times before completely stopping.

If a critical pager notification is received, the On-Call DBA will manually inspect the Control-M Job status by reviewing the available job log output files for the cause of the error. Typically, the log will contain the cause of the failure and will be helpful for troubleshooting and issue resolution.

Enterprise MuleSoft Services (EMS) Application Program Interface

EMS is built on the FedRAMP approved, Workplace.gov Community Cloud-High (WC2-H) AWS PaaS offering. EMS supports secure data transfers between Treasury systems and internal/external applications. The MuleSoft data plane (on WC2-H) is connected to the Anypoint FedRAMP GovCloud system for the purpose of API based management. This implementation of EMS combines on-premise data centers with the Anypoint GovCloud Moderate to support a Hybrid MuleSoft implementation. Integration applications are deployed from the Anypoint Platform Runtime Manager cloud console and are hosted on WC2 hosted Mule servers. Hybrid deployment architecture provides flexibility and control over on-premises security but requires Treasury to provide the hosting infrastructure. EMS does not store any application data within the platform – it is a transient pass-through to fetch/update data from backend systems (ex: HRConnect).

Treasury HRConnect APIs are secure REST APIs that allow API consumers, such as USA Staffing, IRS and other bureaus to transmit data to and receive data from HRConnect. Data is transmitted using secure protocols via near-real time API (application program interfaces) implementations. API connections are brokered using the Treasury Enterprise MuleSoft Services (EMS) System (Treasury MuleSoft High – FIPS High Designation) to backend systems such as

HRConnect and GSA USAccess. Customers use Treasury HRConnect APIs deployed in EMS MuleSoft to fetch or update data in HRConnect.

Integrated Talent Management (ITM)

The Integrated Talent Management (ITM) system receives data from HRConnect. The ITM Product team validates the Learning User Connector - Federal, Learning Organization Connector, and Learning User Connector-SF all run successfully in ITM each morning Monday-Friday to ensure the organizational and user data from HRConnect was successfully added to ITM Learning. In the rare instance the connector fails, SAP NS2 is both emailed and contacted through their ticketing system. An incident is also posted on the EA Incident Reporting Hub. If the connector is run again on the same day, there is no lapse in information passing from HRConnect to ITM.

All ITM accounts are automatically created from HRConnect's user data, and no ITM accounts are manually created or deleted. Only EA can connect to the vendor server. The vendor server cannot initiate a connection to the EA border server. The files are encrypted with the vendor's Pretty Good Privacy (PGP) key before being transferred to the vendor. Encrypted SFTP sessions are used to transfer files. PKI is used to authenticate to the vendor server. Files are encrypted 'at rest' on the HRConnect server using Oracle storage area network (SAN) encryption technologies.

Accuracy Testing Methods

The ITM Program acts as a custodian for customer data housed within the application and is not responsible for its accuracy or integrity; that responsibility belongs to the bureau specific administrators. This nuance applies to the data that ITM inherits via the HRConnect core data feed, and other existing integrations. In the event a data error is identified by the bureau administrators, the process for correction is also inherited from HRConnect. It is the responsibility of the participating agency's process owner to take appropriate steps to correct the findings. Follow-up communication with customers regarding issues is via email.

The successful transmission of the data is validated by daily monitoring of the SAP NS2 SFTP, where inbound files are deposited by the EA border server. The absence of a file indicates a failure of the process. To remediate the issue, the ITM program reports the issue to both HRC and SAP NS2 via tickets followed by escalation via email. Individual incidents caused by timing issues or errors processing the data are resolved and addressed in the next overnight file. Complex issues that result in long term disruptions to the flow of data, are communicated to customers via email along with root cause analysis information and a plan of action to remedy.

ITM Change Control Board

If a change request affects the HRConnect data feed, an in-take request is created with HRConnect to follow the HRConnect intake processes.

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
7.1	Data from HRConnect is received by the Integrated Talent Management (ITM) system. If connector fails, NS2 is both emailed and contacted through their ticketing system. An incident is also posted on the EA Incident Reporting Hub.	Inquired with EA personnel to determine the process for monitoring and control of transmission of data between the ITM and HRConnect. Inspected relevant policies and procedures for monitoring and control of transmission of data to identify specific procedures related to the transferring organizational and user data from HRConnect to ITM to determine the process is defined and documented. For a sample of failed connector incidents, determined whether NS2 received notifications through email.	**No exceptions noted.**
7.2	Files are encrypted in transit and at rest.	Inquired with EA personnel to determine the process for encrypting files before transferring to vendors and when the files are at rest. Inspected relevant policies and procedures regarding encryption of files for HRConnect to determine EA has defined and documented requirements for file encryption in transit and at rest. Inspected the configuration settings of encryption used for both files in transit and files at rest to determine they were configured in accordance with EA requirements.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
7.3	All proposed changes to the ITM system are submitted as a ServiceNow ticket. A CCB meeting is held monthly for customers, stakeholders, and owners to discuss system changes, potential improvements, and efficiencies regarding the requests.	Inquired with EA personnel to determine the ITM change request process (HRConnect in-take processes) including documentation and approval requirements. Inspected relevant configuration management policies and procedures to determine requirements for ITM system changes including the CCB approval process are defined and documented For a sample of closed change tickets related to the HRConnect Data Feed, determined if sampled changes have in-take requests created and went through CCB approval.	**No exceptions noted.**

Control Objective 8: Customer Interagency Agreements

Controls provide reasonable assurance that Customer Interagency Agreements are appropriately monitored in accordance with established procedures to ensure efficiency and performance results.

Description of Controls

EA establishes an Interagency Agreement (IAA) with the Requesting Agency requesting services performed by EA's Shared Services Programs (SSP) and the Department of Treasury. The IAA conforms to the government-wide guidance prescribed by the Bureau of the Fiscal Service (Fiscal Service) in *Treasury Financial Manual*, Vol. I, Part 2, Ch. 4700, App. IO, (May 2019). The IAA authorizes SSP to provide the Requesting Agency service as described in the service description(s).

Each year, EA works closely with its customers to agree on the scope and nature of services to be provided by EA. Customer responsibilities in addition to EA responsibilities are captured within the IAA. EA documents changes to the IAA using form 7600 A&B, General Terms and Conditions (GT&C), and Order, as well as product-specific addenda.

EA's customers are provided the opportunity to participate in survey polls conducted by Treasury. EA performs an annual HRConnect Customer Satisfaction Survey where EA determines the survey timeline and content for the year. The schedule for this survey is shared with the customers during the Customer Collaboration Board (CCB) meeting prior to the survey start date. These survey results are summarized and presented during the subsequent CCB meeting.

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
8.1	EA has Interagency Agreements (IAA) with all non SSP Customers utilizing EA products and services. Customer and EA responsibilities are captured within the IAA. Mid-year changes to the IAA require modifications to the form 7600 A&B, GT&C, and Order. SSP customers utilize an internal transfer process to exchange funds.	Inquired with EA personnel regarding the interagency agreements established by EA SSP to determine the process conforms to the government-wide guidance prescribed by the Bureau of the Fiscal Service in TFM, Vol. I Part 2, Ch 4700, App. IO. Inspected relevant policies and procedures associated with interagency agreements to determine that they define and document customer and EA responsibilities. For a sample of interagency agreements, determined that they conform to government wide guidance prescribed by the Bureau of Fiscal Services and contain both the customer and EA responsibilities. None of the agreements included mid-year changes.	**No exceptions noted.**
8.2	EA performs an annual HRConnect Customer Satisfaction Survey where EA will determine the survey timeline and content for the year. Schedule for survey is shared with customers during the configuration control board (CCB) meeting prior to the survey start date. Survey results are summarized and presented during the subsequent CCB meeting.	Inquired with EA personnel regarding the HRConnect Customer Satisfaction survey to determine the survey timeline and content for the year. Inspected the schedule for the survey to determine the date the survey was shared with customers during the CCB meeting prior to the start of the survey start date. Inspected the configuration control board meeting presentation slides to determine the agenda and results of surveys were discussed during the monthly configuration control board meetings.	**No exceptions noted.**

Control Objective 9: Secure Interface Processes

Controls provide reasonable assurance that processes are in place to establish secure interfaces.

Description of Controls

Enterprise MuleSoft Services (EMS) Application Program Interface

EMS platform running WC2 FedRAMP high cloud hosts API applications developed using MuleSoft technology to mediate integrations between HRConnect and internal and external partner systems. These application fetch/update HRConnect data using Hypertext Transfer Protocol Secure (HTTPS)/Transport Layer Security (TLS) V1.2 protocol. Data traversing through AWS GovCloud and Treasury networks is encrypted and secured through Treasury-WC2H Internet Protocol Security (IPSec) tunnel and Treasury-OCI IPSec tunnel. MuleSoft servers running on WC2-High platform operate using FIPS-140-2 standard security model - data at rest and data in transit are secured and encrypted. Application log files generated in MuleSoft are ingested into Splunk and are preserved for search, reporting and analytics. In addition, all passwords/keys used in MuleSoft applications are secured using client_id/client_secret or oauth 2.0 tokens.

Border Servers

The HRConnect border server securely exchanges interface files between HRConnect and customer agencies. The border server provides special security measures to ensure that all files are scanned for malware and are only accessible by approved individuals.

Customer agencies place their interface files in a specified directory in the customer agency server. The customer agency accesses the HRConnect border server to pull or push interface files. For our file-based interfaces with the IRS, HRConnect uses automated batch processes that transfer files to the IRS Axway service. This transfer takes place between the HRConnect border server and the Axway server using SSH key based authentication and the SFTP protocol.

For customer agencies who contracted with a third-party hosting vendor to transfer interface files, HRConnect uses an automated process to push or pull interface files with the hosting vendor. The third-party hosting vendor does not have access privileges to HRConnect border server.

Only the Secure File Transfer Protocol (SFTP) protocol is support for file transfers. The exception to this rule is that interfaces with the NFC currently use File Transfer Protocol (FTP). The NFC is undergoing a project to implement SFTP. Once implemented, HRConnect will switch to SFTP with the NFC.

Secured Interface

New interface requests are handled through the EA HRConnect change control process. Enterprise Applications Cybersecurity (EAC) team/ISSO/ISSM reviews the change request that includes the information of data to be transmitted to or from HRConnect. The Cybersecurity Team inspects the information to determine whether the data is appropriate and can be adequately secured. The EAC ISSO/ISSM and EA Technical Architecture (TA) meets with the customer agency and third-party vendor, if any, to discuss and identify specific security issues. Once the security issues are resolved, the EAC ISSM approves the customer agency request to begin testing of the connectivity

and transfer of data. When the new interface is approved, the EAC ISSO and ISSM creates an Interconnectivity Security Agreement (ISA) and/or Memorandum of Agreement (MOA) if required. An updated ISA/MOA is required every three years. For any expired ISA, there must be a corresponding POA&M.

The customer agency provides technical contacts to the TA team and to the third-party vendor, if necessary. The customer agency or third-party vendor provides IP addresses of customer agency's data required to transmit the data to the EA border servers (both test and production EA border servers). The EA Deployment team provides the Customer agency's technical contact with an EA Access Request Form.

The EA TA team prepares a maintenance plan to update firewall rules to permit transmission between the customer agency's third-party vendor order servers and EA border servers.

Data exchanges with third-party vendors are encrypted at rest using the recipient's PGP public key. For example, data sent from the border server to the vendor is encrypted at rest using the vendor's public PGP key. For data retrieved from the vendor and placed on the border server, the data is encrypted at rest using the HRCPO public PGP key.

The EA TA team establishes password-based connectivity to the third-party vendor servers using SFTP and the newly provided credentials. Then the EA TA team provides the Treasury SSH public key to the partner and requests that they add the Treasury public key to the partner's PKI KeyStore. Once this is completed, the EA TA team can establish key-based authentication instead of password-based authentication. Once key-based authentication is established, the EA TA team automates the file transfer process. The EA Deployment team provides the connectivity information (Unix ID and password, EA border server name/IP address, and Linux directory where interface files are stored) to the Customer agency's technical contact.

The EA TA team and third-party vendor test the basic file transfers and PGP encryption/ decryption capabilities.

The EA developer responsible for the interface program creates a ClearQuest Technical Architecture (CQ TA) Work Order to have Control-M automate the pushing and pulling of files between the Control-M server and the EA border server. The TA Work Order contains information including the names of the files being transferred, the size of the files being transferred, and the transfer schedule. The EA developer refers to the CQ TA Work Order in the interface program Object Migration Request (OMR) migration notes so that the Control-M updates are made at the same time as the interface program is migrated.

The EAC ISSO/ISSM reviews the production implementation, and file transfer automation is enabled in production.

Complementary Customer Agency Controls

Customer agency auditors should determine whether customer agencies have established controls to provide reasonable assurance that the Customer agency's technical contact tests connectivity from the Customer agency's border server to the EA border server using SSH and SFTP. It is recommended, but not required that the Customer agency's technical contact places the Customer agency's border server public key on the EA border server so that certificate-based authentication can take place. The Customer agency's technical contact should also test file transfers (pushes and pulls) between the Customer agency's border server and the EA border server.

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
9.1	New interface requests are managed through the EA Intake Process. The EA Cybersecurity Team/ISSO reviews the change request that includes the information of data to be transmitted to or from HRConnect. When the new interface is approved, the EA Cybersecurity team creates an Interconnectivity Security Agreement (ISA) and/or Memorandum of Agreement (MOA) if required.	Inquired with EA Cybersecurity Team to obtain an understanding of the EA HRConnect change control process for interface requests and authorization among interface partners. Inspected relevant policies and procedures to determine the EA requirements for interface management are defined and documented. For a sample of new ISAs, Obtained and inspected evidence to determine whether the sampled new interfaces were approved by the EA Cybersecurity Team and also the correspondent ISA and/or MOAs are created.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
9.2	EA reviews and updates ISA/MOAs every three years. For any expired ISA, there must be a corresponding POA&M.	Inquired with EA to determine how ISA/MOA reviews are performed. Inspected relevant policies and procedures to determine they outlined the process of reviewing and updating ISA/MOAs. Inspected the latest management review evidence to determine EA reviewed and updated the ISA/MOAs every three years. For a sample of expired ISAs, Obtained and inspected evidence showing that any expired ISAs have a related POA&M to ensure the ISA is being tracked until it is resolved/renewed.	**No Exception Noted.**
9.3	The EA Deployment team provides the Customer agency's technical contact with an EA Access Request Form if the customer agency provides technical contacts to the TA team and to the third-party vendor as necessary. The customer agency or third-party vendor provides IP addresses of customer agency's data required to transmit the data to the EA border servers (both test and production EA border servers). The EA TA team then creates a Fiscal Services Change Request (CR) requesting the Fiscal Services update firewall rules to allow the transmission between the customer agency or third-party vendor to the EA border servers.	Inquired with EA personnel to determine the process for transmitting data to EA border servers. Inspected relevant policies and procedures to determine the process for requesting access for transmitting data to EA border servers is defined and documented. For sampled ISAs from Control Number 9.1, obtained and inspected supporting documentation to determine that each of the ISAs had technical contacts, IP addresses, and completed change requests to update firewall rules to allow transmissions between the customer agency or third-party vendor to the EA border servers.	**No exceptions noted.**

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
9.4	EA TA team establishes password-based connectivity to the third-party vendor servers using SFTP and the newly provided credentials. Then the EA TA team provides the Treasury SSH public key to the partner and requests that they add the Treasury public key to the partner's PKI KeyStore. Once this is completed, the EA TA team can establish key-based authentication instead of password-based authentication. Once key-based authentication is established, the EA TA team automates the file transfer process.	Inquired with EA personnel to determine the process for establishing password-based connectivity and providing public keys to interface partners. Inspected relevant policies and procedures to determine the process for establishing password-based connectivity and providing public keys to interface partners is defined and documented. For sampled ISAs from Control Number 9.1, obtained and inspected evidence to determine that SSH and PKI key connectivity was established instead of password-based authentication.	**No exceptions noted.**
9.5	The EA developers are responsible for the interface program creates a ClearQuest Technical Architecture (CQ TA) Work Order to have Control-M automate the pushing and pulling of files between the Control-M server and the EA border server. The TA Work Order contains information including the names of the files being transferred, the size of the files being transferred, and the transfer schedule. The EA developer refers to the CQ TA Work Order in the interface program Object Migration Request (OMR)migration notes so that the Control-M updates are made at the same time as the interface program is migrated.	Inquired with EA personnel to determine the process of creating work orders for Control-M and the approval process for production implementation. Inspected relevant policies and procedures to determine the process of creating work orders for Control-M and the approval process for production implementation are defined and documented. For sampled ISAs from Control Number 9.1. Obtained and inspected supporting documentation for the sample to determine Control-M job scheduling was established for automatically pulling and pushing files.	**No exceptions noted.**

Control Objective 10: Subservice Organizations

Controls provide reasonable assurance that EA monitors subservice organization and tests for compliances with complementary customer agency controls.

Description of Controls

Oracle OMCS and OCI GovCloud Cloud Service Provider (CSP)

HRConnect resides upon the Oracle Cloud Infrastructure (OCI) Infrastructure as a Service (IaaS) GovCloud Cloud Service Provider (CSP). Treasury EA reviewed the FedRAMP SA&A package and issued a Treasury Agency authorization to use the OCI IaaS High GovCloud CSP December 6, 2019. Treasury also provided a FedRAMP-based ATO of OCI IaaS High GovCloud. HRConnect (on OCI) obtained its formal Agency Authority to Operate (ATO) January 31, 2020. Oracle OCI High GovCloud received its FedRAMP Provisional ATO (pATO) 4/10/2020. Treasury ended its formal sponsorship of OCI IaaS GovCloud once the FedRAMP PMO issued its pATO of OCI IaaS (see https://marketplace.fedramp.gov).

EAC reviews OCI's FedRAMP Continuous Monitoring information via monthly ConMon meetings and annually via OCI IaaS SA&A package reviews when the documentation is provided by Oracle. OMCS is the division within Oracle that manages the O&M for the HRConnect application.

National Finance Center

EA reviews SSAE 18 results or other control-related documentation provided by subservice organizations to determine whether deficiencies (if any) affect subservice organization controls that in turn may impact the related financial reporting of HRConnect systems. The EA EAC annually reviews interconnected subservice organizations' systems' SSAE18 and Security Assessment and Authorization (SA&A) documentation to review an interconnected system's FISMA status.

Complementary Customer Agency Controls

Customer agency has established controls to provide reasonable assurance that SINQ errors, HCUP Status, and mismatch cases are corrected to ensure transactions are processed correctly. The customer agency has also established controls to provide reasonable assurance that data sent and received within the HRConnect system is applicable and accurate.

#	Description of Controls Provided by Information Operations (EA)	Tests of Design and Operating Effectiveness Performed (S&R)	Results of Design and Operating Effectiveness Testing (S&R)
10.1	Oracle OCI GovCloud Cloud Service Provider (CSP) Treasury EA reviewed the FedRAMP SA&A package and issued a Treasury Agency ATO of the OCI IaaS High GovCloud CSP. Treasury EA monthly and annually reviews ConMon and SA&A documentation of the OCI IaaS High GovCloud CSP.	Inquired with EA personnel to determine the process for monitoring Oracle OCI for compliance. Inspected the results of Treasury EA's review of the FedRAMP SA&A package to determine a Treasury Agency ATO was issued for the CSP. For a sample of monthly reviews of ConMon and SA&A documentation of the CSP, ensured they were performed in accordance with Treasury requirements. Inspected the results of the annual review of ConMon and SA&A documentation of the CSP to ensure it was performed in accordance with Treasury Requirements.	**Exception Noted – ConMon Review (NFR 2)** EA did not perform its monthly ConMon meeting to review OCI FedRAMP ConMon information for the month of December 2024.
10.2	EA reviews the National Finance Center (NFC) SSAE 18 report, SA&A documentation, and other subservice organization related documentation.	Inquired with EA personnel to determine the process for monitoring controls of subservice organizations. Inspected NFC subservice organization monitoring evidence to determine that EA reviewed NFC's SSAE 18 report, SA&A documentation, and other subservice organization related documentation in accordance with EA Requirements.	**No exceptions noted.**

V: OTHER INFORMATION PROVIDED BY THE MANAGEMENT OF ENTERPRISE APPLICATIONS

RESPONSES FROM MANAGEMENT TO FINDINGS IDENTIFIED

Response to NFR 1 – Database Scans
The Enterprise/DO Cybersecurity team is working to promptly restore operational status of the DBProtect scanning tool to ensure timely vulnerability detection and mitigation across affected databases. To prevent future disruptions, the team will document and enforce backup procedures or mitigating controls in the event of similar system failures.

Additionally, the team is actively working to establish a trust relationship between HRConnect and Treasury Cloud, which is a critical technical prerequisite for enabling DBProtect scans to resume successfully and securely.

☒ Management concurs with the finding and recommendation.
☐ Management does not concur with the finding and recommendation.

Response to NFR 2 – ConMon Review
A secondary individual, Alternate ISSO (AISSO) will be formally designated to serve as the backup reviewer for monthly ConMon activities. This individual will be empowered to assume responsibilities in the absence of the ISSO to ensure continuity of monitoring activities and compliance with FedRAMP requirements. Formal training will be provided to AISSO to ensure they have the knowledge and capability necessary to perform comprehensive reviews of OCI FedRAMP continuous monitoring reports.

Treasury Enterprise Applications will update internal SOPs to reflect the AISSO role and ensure appropriate delegation of responsibilities (POA&M ID: IPT0075474). Documentation will identify the designated individual and clearly define expectations for performing ConMon reviews when the ISSO is unavailable. Treasury Enterprise Applications will coordinate with Enterprise/DO Cybersecurity to develop or provide existing training for the AISSO. This training will include review procedures, assessment methodologies, and documentation standards consistent with FedRAMP guidance and Treasury's information security policies.

☒ Management concurs with the finding and recommendation.
☐ Management does not concur with the finding and recommendation.

REPORT WASTE, FRAUD, AND ABUSE

Submit a complaint regarding Treasury OIG Treasury Programs and Operations using our online form: https://oig.treasury.gov/report-fraud-waste-and-abuse

TREASURY OIG WEBSITE

Access Treasury OIG reports and other information online: https://oig.treasury.gov/